# 天珣内网安全风险管理与审计系统 用户手册

(V6.6.9.4Patch66940000)



## 启明星辰

Beijing Venustech Cybervision Co., Ltd.

2012 年 11 月



## 版权声明

# 北京启明星辰信息安全技术有限公司版权所有,并保留对本手册及本声明的最终解释权和修改权。

本手册中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容,除另有特别注明外,其著作权或其他相关权利均属于北京启明星辰信息安全技术有限公司。未经 北京启明星辰信息安全技术有限公司书面同意,任何人不得以任何方式或形式对本手册 内的任何部分进行复制、摘录、备份、修改、传播、翻译成其它语言、将其全部或部分 用于商业用途。本文档中的信息归北京启明星辰信息安全技术有限公司所有并受著作权 法保护。

"天珣"为北京启明星辰信息安全技术有限公司的注册商标,不得仿冒。

#### 信息更新

本文档及其相关计算机软件程序(以下文中称为"文档")仅用于为最终用户提供信息,并且随时可由北京启明星辰信息安全技术有限公司(下称"启明星辰")更改或撤回。

#### 免责声明

本手册依据现有信息制作,其内容如有更改,恕不另行通知。

北京启明星辰信息安全技术有限公司可能已经拥有或正在申请与本文档主题相关的各项专利。提供本文档并不表示授权您使用这些专利。您可将许可权查询资料用书面方式寄往北京启明星辰信息安全技术有限公司。

北京启明星辰信息安全技术有限公司在编写该手册的时候已尽最大努力保证其内容准确可靠,但北京启明星辰信息安全技术有限公司不对本手册中的遗漏、不准确、或错误 导致的损失和损害承担责任。

#### 出版时间

2012年12月20日



目 录

(V	6.6.9	9.4PATCH66940000)	1
1.	体系	结构	1
1.1	. 「	中心服务器、本地服务器、客户端、以及策略网关的体系结构	1
1.2	. <u>;</u>	系统中的角色及术语	1
	1.2.1.	,  角色	1
	1.2.2.	术语	2
2.	WE	B 控制台登录	3
2.1	. =	关于 WEB 控制台登录	3
2.2	2. 1	WINDOWS 集成认证登录页面	4
-	2.2.1.	配置介绍	4
	2.2.2.	配置要点	4
2.3	). <u>-</u>	三权分立认证登录页面	5
	2.3.1.	配置介绍	5
	2.3.2.	配置要点	7
3.	首页		8
4	基木	· 而 署	0
т	<u>45</u> 47		)
4.1	. 5	关于基本配置	9
4.2	2. ]	按需支援操作员	11
4	4.2.1.		11
4.2	4.2.2.		12
4.5	). 4 0 1	系统官理贝 町 四 ヘ / 加	12
2	4.3.1. 4 2 2		12
1 1	+.⊃.∠. I 4	·	.13
4.4	••••••••••••••••••••••••••••••••••••••	<b>來哘脉労奋</b>	<b>10</b>
4 5	+.+.1. ; 4	· 印里月知····································	10
	,. 451	回至174 <b>久</b> 	18
4	4.5.2.		20
4.6	5. I	IP 组	21
2	4.6.1.		21
4.7		部门	26
2	4.7.1.	配置介绍	26
4.8	i. ź	终端注册	28
2	4.8.1.	配置介绍	28
4.9	). 7	本地用户	30
2	4.9.1.	配置介绍	30
4.1	0.	用户组	32
4	4.10.1	1. 配置介绍	32
4	4.10.2	2. 配置要点(以 AD 域为例)	38



4.1	11.	可信	<b>第 MAC</b>	39
	4.11.	1.	配置介绍	39
	4.11.	2.	配置要点	42
4.1	12.	Ц	「信 GUID	43
	4.12.	1.	配置介绍	43
	4.12.	2.	配置要点	45
4.1	13.	乕	]户、IP、MAC 组合	45
	4.13.	1.	配置介绍	45
	4.13.	2.	配置要点	54
4.1	14.	XX	列络设备配 <u>置</u>	55
4.1	15.	分	▶组信息	58
	4.15.	1.	配置介绍	58
4.1	16.	全	≥局参数	58
	4.16.	1.	配置介绍	58
5.	安全	基	线	64
5.1	1.	关于	-安全基线	64
5.2	2.	入す	- みと思え、	66
	5.2.1		配置介绍	66
	1.1.1	•	配置要点	69
5.3	3.	进租	是运行策略	70
	5.3.1		配置介绍	70
5.4	4.	软件	安装策略	75
	5.4.1		配置介绍	75
5.5	5.	WIN	NDOWS 服务管理	80
:	5.5.1		配置介绍	80
5.6	6.	防病	<b>5毒软件策略</b>	83
	5.6.1	•	配置介绍	83
5.7	7.	WIN	DOWS 账户策略	85
:	5.7.1	•	配置介绍	85
5.8	8.	WIN	DOWS 本地策略	90
	5.8.1	חר גרי	配直介绍	90 9 <b>7</b>
5.9	<b>9.</b> :	<b>壮</b> 苁		97
5 1	5.9.1 10	++	<b>℡直</b> 介瑫	97
5.1	5 10	・ 1	<b>学页源目连</b> 	<b>99</b>
5 1	5.10. 11	1. Win	1. 1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	99 AA
5.1	<b>5</b> 11	** <b>⊥</b> \ 1 ₹	wows 尹山口心自姓水町 ····································	00
5 1	5.11. 12	⊥ ⊧ Æ	1 1 1 1	02
	5.12.	1.	配置介绍	02
6.	准入	、 控f	制11	10
		-у-с. т - ү-с. т	· · · · · · · · · · · · · · · · · · ·	10
6.] 4 1	1. : >	大寸	1出八江中JⅠ 22准 λ	1U 11
0.2	<b>≟.</b> 621	M绐	ημ//I 关于网络准λ 1	<b>11</b>
	J.4.1	•	/ 、 4 1 4-日1 臣/ 入	<b>T T</b>



6.2.2.	RADIUS Server 页面	112
6.2.3.	可信 MAC 认证实时授权页面	119
6.2.4.	可信 GUID 认证实时授权页面	
6.2.5.	免认证 MAC 地址列表页面	
6.2.6.	VLAN 信息页面	
6.2.7.	网络准入配置要点	
6.2.8.	网络准入其他组件配置	
6.3. 应	用准入	
6.3.1.	关于应用准入	
6.3.2.	策略网关代理设置页面	
6.3.3.	中性(通用)策略网关安装配置要点	
6.3.4.	旁路 DNS 准入	167
6.3.5.	IIS 策略网关安装配置要点	
6.3.6.	ISA 策略网关安装配置要点	
6.3.7.	Exchange 策略网关安装配置要点	
6.3.8.	Web 准入安装配置要点	
6.4. 客	户端准入	
6.4.1.	关于客户端准入	
6.4.2.	客户端准入页面	
6.5. Al	RP 准入	
6.5.1.	关于 ARP 准入	
6.5.2.	ARP 准入页面	
7. 安全防	方护	
7. 安全隊 7.1. 关	方护 于安全防护	
7. 安全 <b>阶</b> 7.1. 关 7.2. 协	方护 于安全防护 议端口设定	
<b>7.</b> 安全防 <b>7.1.</b> 关 <b>7.2.</b> 协 7.2.1.	方护 于安全防护 议端口设定 配置介绍	
7. 安全阶 7.1. 关 7.2. 协 7.2.1. 7.3. 防	方护 于安全防护 议端口设定 配置介绍 护策略	
7. 安全网 7.1. 关 7.2. 协 7.2.1. 7.3. 防 7.3.1.	方护 于安全防护 ·议端口设定 配置介绍 护策略 配置介绍	
7. 安全的 7.1. 关 7.2. 协 7.2.1. 7.3. 防 7.3.1. 7.3.2.	方护 于安全防护 议端口设定 配置介绍 护 <b>策略</b> 配置介绍 配置介绍	
7. 安全的 7.1. 关 7.2. 协 7.2.1. 7.3. 防 7.3.1. 7.3.2. 7.4. 访	方护 于安全防护 ·议端口设定 配置介绍 护策略 配置介绍 配置实点 客策略	<b>185 185 186 186 189</b> 189200 <b>201</b>
7. 安全的 7.1. 关 7.2. 协 7.2.1. 7.3. 防 7.3.1. 7.3.2. 7.4. 访 7.4.1.	方护	
<ol> <li>7. 安全阶</li> <li>7.1. 关</li> <li>7.2. 协</li> <li>7.2.1.</li> <li>7.3. 防</li> <li>7.3.2.</li> <li>7.4. 访</li> <li>7.4.1.</li> <li>8. 补丁管</li> </ol>	方护 于安全防护 议端口设定 配置介绍 配置介绍 配置介绍 配置要点	
<ol> <li>7. 安全阶</li> <li>7.1. 关</li> <li>7.2. 协</li> <li>7.2.1.</li> <li>7.3. 防</li> <li>7.3.2.</li> <li>7.4. 访</li> <li>7.4.1.</li> <li>8. 补丁管</li> <li>8.1. 关</li> </ol>	方护 于安全防护 议端口设定 配置介绍 配置介绍 配置要点 配置外绍	
<ol> <li>7. 安全网</li> <li>7.1. 关</li> <li>7.2. 协</li> <li>7.2.1.</li> <li>7.3. 防</li> <li>7.3.2.</li> <li>7.4. 访</li> <li>7.4.1.</li> <li>8. 补丁管</li> <li>8.1. 关</li> <li>8.2. 在</li> </ol>	方护	
<ol> <li>安全网</li> <li>7.1、 关</li> <li>7.2. 协</li> <li>7.2.1.</li> <li>7.3. 防</li> <li>7.3.2.</li> <li>7.4. 访</li> <li>7.4.1.</li> <li>8. 补丁管</li> <li>8.1. 关</li> <li>8.2. 在</li> <li>8.2.1.</li> </ol>	<ul> <li>方护</li></ul>	
<ol> <li>安全网</li> <li>7.1、关</li> <li>7.2. 协</li> <li>7.2.1.</li> <li>7.3. 防</li> <li>7.3.2.</li> <li>7.4. 访</li> <li>7.4.1.</li> <li>8. 补丁管</li> <li>8.1. 关</li> <li>8.2. 在</li> <li>8.2.1.</li> <li>8.2.2.</li> </ol>	<ul> <li>方护</li></ul>	
<ol> <li>安全网</li> <li>7.1、 关</li> <li>7.2. 协</li> <li>7.2.1.</li> <li>7.3. 防</li> <li>7.3.2.</li> <li>7.4. 访</li> <li>7.4.1.</li> <li>8. 补丁管</li> <li>8.1. 关</li> <li>8.2. 在</li> <li>8.2.1.</li> <li>8.2.2.</li> <li>8.2.3.</li> </ol>	方护	
<ol> <li>安全网</li> <li>7. 安全网</li> <li>7.1. 关</li> <li>7.2. 协</li> <li>7.3. 防</li> <li>7.3.1.</li> <li>7.3.2.</li> <li>7.4. 访</li> <li>7.4.1.</li> <li>8. 补丁管</li> <li>8.1. 关</li> <li>8.2. 在</li> <li>8.2.1.</li> <li>8.2.3.</li> <li>8.3. 手</li> </ol>	方护	
<ol> <li>安全例</li> <li>7.1、 关</li> <li>7.2. 协</li> <li>7.2.1.</li> <li>7.3. 防</li> <li>7.3.1.</li> <li>7.3.2.</li> <li>7.4. 访</li> <li>7.4.1.</li> <li>8. 补丁管</li> <li>8.1. 关</li> <li>8.2. 在</li> <li>8.2.1.</li> <li>8.2.2.</li> <li>8.2.3.</li> <li>8.3. 手</li> <li>8.3.1.</li> </ol>	方护 5. 于安全防护 5. 议端口设定 配置介绍 2. 配置介绍 2. 配置夹点 3. 密策略 2. 配置介绍 5. 并丁管理 5. 关于在线补丁源 美于在线补丁源 正置 介绍 二 和丁源 关于手工补丁源	
<ol> <li>安全网</li> <li>7. 安全网</li> <li>7.1. 关</li> <li>7.2. 协</li> <li>7.3. 防</li> <li>7.3.1.</li> <li>7.3.2.</li> <li>7.4. 访</li> <li>7.4.1.</li> <li>8. 补丁管</li> <li>8.1. 关</li> <li>8.2. 在</li> <li>8.2.1.</li> <li>8.2.3.</li> <li>8.3. 手</li> <li>8.3.1.</li> <li>8.3.2.</li> </ol>	<ul> <li>方护</li> <li>示于安全防护</li> <li>议端口设定</li> <li>配置介绍</li> <li>配置介绍</li> <li>配置介绍</li> <li>配置介绍</li> <li>常理</li> <li>子补丁管理</li> <li>线补丁源</li> <li>关于在线补丁源</li> <li>配置介绍</li> <li>配置子ゴッ</li> </ul>	
<ol> <li>安全网</li> <li>7. 安全网</li> <li>7.1. 关</li> <li>7.2. 协</li> <li>7.2.1.</li> <li>7.3. 防</li> <li>7.3.2.</li> <li>7.4. 访</li> <li>7.4.1.</li> <li>8. 补丁管</li> <li>8.1. 关</li> <li>8.2. 在</li> <li>8.2.1.</li> <li>8.2.2.</li> <li>8.2.3.</li> <li>8.3.5</li> <li>8.3.1.</li> <li>8.3.2.</li> <li>8.4. 补</li> </ol>	方护 于安全防护 心端口设定 配置介绍 的第略 配置介绍 配置介绍 家策略 配置介绍 常理 专并打管理 关于在线补丁源 美于在线补丁源 配置介绍 而置介绍 而置介绍 而置介绍 而置介绍 而置介绍 而置介绍 方另介绍 新丁次	
<ol> <li>安全网</li> <li>7. 安全网</li> <li>7.1. 关</li> <li>7.2. 协</li> <li>7.2.1.</li> <li>7.3. 防</li> <li>7.3.2.</li> <li>7.4. 访</li> <li>7.4.1.</li> <li>8. 补丁管</li> <li>8.1. 关</li> <li>8.2. 在</li> <li>8.2.1.</li> <li>8.2.3.</li> <li>8.3.5 手</li> <li>8.3.1.</li> <li>8.3.2.</li> <li>8.4. 补</li> </ol>	方护 于安全防护 议端口设定 配置介绍 配置介绍 配置介绍 配置齐昭 配置介绍 考策略 配置介绍 考理 关于在线补丁源 美于在线补丁源 配置介绍 配置介绍 配置介绍 表于子本丁源 和丁第 大于手工补丁源 而置子介绍 方绍 方绍 方名	185         185         186         186         189         189         200         201         201         201         201         201         201         201         205         206         207         213         214         214         214         214         214         214         214         214         214         216



8.5.	WSUS 集成管理	
8.6.	关于 WSUS 集成管理	
8.6.1	I. 配置介绍	
8.6.2	2. 配置要点	
8.7.	补丁查询	
8.7.1	l. 关于补丁查询	
8.7.2	2. 配置介绍	
9. 资产	∽管理	
0.1	<u>,</u> 半二次立体理	224
9.1.	大丁页厂官理	
<b>10.</b> 키	■法外联	
10.1.	关于非法外联	
10.2.	非法外联监控	
10.2	.1. 配置介绍	
10.3.	多网卡限制	
10.4.	关于多网卡限制	
10.4	.1. 多网卡限制页面	
10.5.	拨号限制	
10.5	.1. 关于拨号限制	
10.5	.2. 拨号限制页面	
10.6.	外设管理	
10.6	.1. 关于外设管理	
10.6	.2. 外设管理页面	
10.7.	异常路由审计	
10.7	.1. 关于异常路由审计	
10.7	.2. 异常路由审计配置页面	
11. 移	多动存储	
11.1.	关于移动存储	245
11.2.	设备认证策略	
11.2	2.1. 关于设备认证策略	
11.2	.2. 移动存储设备提交认证相关	页面
11.3.	移动存储设备管理页面	
11.4.	设备授权	
11.4	.1. 关于设备授权	
11.4	.2. 移动存储设备授权页面	
11.5.	可使用未认证设备的计算机	
11.6.	分区解扰操作说明	
12. 丝	&端审计	
12.1	关于终端宙计	261
12.2	文件宙计及控制策略	201 263
12.2	.1 关于文件审计及控制策略	263
12.3.	文件审计及控制策略	



13.2.1	关于文件审计及控制策略	
12.2.2	文件操作审计及控制页面	
12.2.3	审计网络拷贝页面	
12.4.	打印审计及控制	
12.3.1	关于打印审计	
12.3.2	打印审计页面	
12.5.	网站审计及控制	
12.4.1	网站审计及控制页面	
12.6.	FTP 审计及控制	
12.5.1	FTP 审计及控制页面	
12.7.	文件涉密信息审计	
12.6.1	文件涉密信息审计页面	
12.6.2	附录 1	
12.8.	应用程序使用审计	
12.7.1	应用程序使用审计页面	
12.9.	刻录审计	
12.8.1	刻录审计策略页面	
12.10.	WINDOWS 事件日志审计	
12.9.1	Windows 事件日志审计页面	
13. 桌面	面运维	
13.1	关于卓面运维	291
10.11		
13.2.	软件分发	
<b>13.2.</b> 13.2.1.	<b>软件分发</b>	<b>291</b>
<b>13.2.</b> 13.2.1. 13.2.2.	<b>软件分发</b>	<b>291</b> 291 292
<b>13.2.</b> 13.2.1. 13.2.2. 13.2.3.	<b>软件分发</b> 关于软件分发 软件分发设置页面	<b>291</b> 291 292 296
<b>13.2.</b> 13.2.1. 13.2.2. 13.2.3. 13.2.4.	<b>软件分发</b> 关于软件分发 软件分发设置页面	<b>291</b> 291 292 296 297
<b>13.2.</b> 13.2.1. 13.2.2. 13.2.3. 13.2.4. <b>13.3.</b>	<b>软件分发</b> 关于软件分发 软件分发设置页面	
<b>13.2.</b> 13.2.1. 13.2.2. 13.2.3. 13.2.4. <b>13.3.</b> 13.3.1.	<b>软件分发</b>	
<b>13.2.</b> 13.2.1. 13.2.2. 13.2.3. 13.2.4. <b>13.3.</b> 13.3.1. 13.3.2.	<b>软件分发</b>	
<b>13.2.</b> 13.2.1. 13.2.2. 13.2.3. 13.2.4. <b>13.3.</b> 13.3.1. 13.3.2. <b>13.4.</b>	<b>软件分发</b>	
<b>13.2.</b> 13.2.1. 13.2.2. 13.2.3. 13.2.4. <b>13.3.</b> 13.3.1. 13.3.2. <b>13.4.</b> 13.4.1.	<b>软件分发</b>	
<b>13.2.</b> 13.2.1. 13.2.2. 13.2.3. 13.2.4. <b>13.3.</b> 13.3.1. 13.3.2. <b>13.4.</b> 13.4.1. 13.4.2.	<b>软件分发</b>	
<b>13.2.</b> 13.2.1. 13.2.2. 13.2.3. 13.2.4. <b>13.3.</b> 13.3.1. 13.3.2. <b>13.4.</b> 13.4.1. 13.4.2. 13.4.3.	软件分发	
<b>13.2.</b> 13.2.1. 13.2.2. 13.2.3. 13.2.4. <b>13.3.</b> 13.3.1. 13.3.2. <b>13.4.</b> 13.4.1. 13.4.2. 13.4.3. 13.4.4.	软件分发	
<b>13.2.</b> 13.2.1. 13.2.2. 13.2.3. 13.2.4. <b>13.3.</b> 13.3.1. 13.3.2. <b>13.4.</b> 13.4.1. 13.4.2. 13.4.3. 13.4.4. <b>13.5.</b>	软件分发	
<b>13.2.</b> 13.2.1. 13.2.2. 13.2.3. 13.2.4. <b>13.3.</b> 13.3.1. 13.3.2. <b>13.4.</b> 13.4.1. 13.4.2. 13.4.3. 13.4.4. <b>13.5.</b> 13.5.1.	<ul> <li>软件分发</li></ul>	
<ul> <li>13.2.</li> <li>13.2.1.</li> <li>13.2.2.</li> <li>13.2.3.</li> <li>13.2.4.</li> <li>13.3.1.</li> <li>13.3.2.</li> <li>13.4.</li> <li>13.4.2.</li> <li>13.4.3.</li> <li>13.4.4.</li> <li>13.5.</li> <li>13.5.1.</li> <li>13.6.</li> </ul>	<ul> <li>软件分发</li></ul>	
<ul> <li>13.2.</li> <li>13.2.1.</li> <li>13.2.2.</li> <li>13.2.3.</li> <li>13.2.4.</li> <li>13.3.1.</li> <li>13.3.2.</li> <li>13.4.</li> <li>13.4.2.</li> <li>13.4.3.</li> <li>13.4.4.</li> <li>13.5.</li> <li>13.5.1.</li> <li>13.6.</li> <li>13.6.1.</li> </ul>	<ul> <li>软件分发</li></ul>	
<ul> <li>13.2.</li> <li>13.2.1.</li> <li>13.2.2.</li> <li>13.2.3.</li> <li>13.2.4.</li> <li>13.3.1.</li> <li>13.3.2.</li> <li>13.4.</li> <li>13.4.2.</li> <li>13.4.3.</li> <li>13.4.4.</li> <li>13.5.</li> <li>13.5.1.</li> <li>13.6.1.</li> <li>13.7.</li> </ul>	<ul> <li>软件分发</li></ul>	
<ul> <li>13.2.</li> <li>13.2.1.</li> <li>13.2.2.</li> <li>13.2.3.</li> <li>13.2.4.</li> <li>13.3.1.</li> <li>13.3.2.</li> <li>13.4.</li> <li>13.4.3.</li> <li>13.4.4.</li> <li>13.5.</li> <li>13.6.</li> <li>13.6.1.</li> <li>13.7.</li> <li>13.7.1.</li> </ul>	<ul> <li>软件分发</li></ul>	
<ul> <li>13.2.</li> <li>13.2.1.</li> <li>13.2.2.</li> <li>13.2.3.</li> <li>13.2.4.</li> <li>13.3.1.</li> <li>13.3.2.</li> <li>13.4.</li> <li>13.4.2.</li> <li>13.4.3.</li> <li>13.4.4.</li> <li>13.5.</li> <li>13.6.1.</li> <li>13.6.1.</li> <li>13.7.1.</li> <li>13.8.</li> </ul>	<ul> <li>软件分发</li></ul>	
<ul> <li>13.2.</li> <li>13.2.1.</li> <li>13.2.2.</li> <li>13.2.3.</li> <li>13.2.4.</li> <li>13.3.1.</li> <li>13.3.2.</li> <li>13.4.</li> <li>13.4.3.</li> <li>13.4.4.</li> <li>13.5.</li> <li>13.6.</li> <li>13.6.1.</li> <li>13.7.</li> <li>13.8.</li> <li>13.8.1.</li> </ul>	<ul> <li>软件分发</li></ul>	
<ul> <li>13.2.</li> <li>13.2.1.</li> <li>13.2.2.</li> <li>13.2.3.</li> <li>13.2.4.</li> <li>13.3.1.</li> <li>13.3.2.</li> <li>13.4.</li> <li>13.4.2.</li> <li>13.4.3.</li> <li>13.4.4.</li> <li>13.5.</li> <li>13.6.1.</li> <li>13.6.1.</li> <li>13.7.1.</li> <li>13.8.</li> <li>13.8.1.</li> <li>13.8.2.</li> </ul>	<ul> <li>软件分发</li></ul>	



13.	.8.4.	网络连接页面	
13.	.8.5.	实时补丁查询页面	
13.	.8.6.	IE 插件管理页面	
13.	.8.7.	终端锁屏	
13.	.8.8.	终端维护	
13.9.		终端资源状况监控	
13.	.9.1.	关于终端资源状况监控	
14	认证	★ 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	310
17. 1	ЮЛ И		
14.1.	•	第三方 CA 机构	
14.2.		大坦 CA 机构	
14.	. 2. 1	. 大珣 CA 根证书	
14.	.2.2.	大珣 CA 用户证书	
14.	.2.3.	天珣 CA 用户证书页面证书及 ActiveX 控件安装	
14.3.	•	身份认证	
14.	.3.1.	关于身份认证	
14.	.3.2.	用户及证书管理配置介绍	
14.	.3.3.	超级用户	
15. 1	信息	中心	
15 1		关于信息中心	333
15.2	•	次,1027-0	334
15.2	21	网里介绍	33/
15.3	.2.1.	□□□/扣 资 <b>产</b> /自	338
15.5	31	页/ 旧心····································	338
15.	.3.1.	电直升和	355
13.4.	11	们了 <b>问心</b>	255
13.4 15.5	.4.1.	—————————————————————————————————————	
15.5.	5 1	甲月宿心	
15.	.5.1.	能直介绍 动人甘体	
15.6.		女王奉残	
15.	.6.1.	配直介绍	
15.7.		外联控制	
15.	.7.1.		
15.8.		攻击告警	
15.	.8.1.	配置介绍	
15.9.		移动存储	
15.	.9.1.	配置介绍	
15.10	).	桌面运维	
15.	.10.1	. 配置介绍	
15.11.	•	级联报表	
15.	.11.1	. 配置介绍	
16.	系约	维护	
16.1.		关于系统维护	
16.2.		系统维护	



16.2.1	. 客户端升级配置页面	
16.2.2	. 自动卸载客户端页面	
16.2.3	. 数据库自动维护	
16.2.4	. 软件分发 IP 组同步	
16.3.	系统日志	
16.3.1	. 管理员操作日志页面	
16.3.2	,按需支援日志页面	
15.2.3	策略服务器日志页面	
15.2.4	告警服务器同步日志页面	
15.2.5	策略网关日志页面	
15.2.6	5 RADIUS 日志页面	
15.2.7	补丁同步日志页面	
16.4.	LICENSE 管理	
16 系统级	及联	
16.1 <del>关<sup>-</sup></del>	千系统级联	437
16.2 级联	关关系。 第关系	438
16.2.1		438
16.3 级耶	关策略管理	
16.3.1	配置介绍	
16.4 授材	又分拆	
16.4.1	配置介绍	
16.5 级国	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
16.5.1	配置介绍	
17 更新策		
171 兰二		113
17.1 天、	」	
17.2 文章	9水町1700年。 Server 等政版太市市	лананананананананананананананананананан
17.3 5	PERVER 宋阳版平贝田 ····································	ллл ЛЛЛ
17.3.1	电重开印。 本	
17.3.2	· 平地派分留床下向了	446
17.4	■ □ □ □ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	
17.4.1	配置介绍	447
17.4.2	配置要占	447
17.5	更新策略网关策略页面	
17.5.1	配置介绍	
17.5.2	配置要点	
17.6	更新 RADIUS 策略页面	
17.6.1	配置介绍	
17.6.2	配置要点	
18. 附表	录:单点登录配置手册	450
18 1	于和单占登录简介	150
18. 2	▲点登录客户端打包	
_ ~	, , , , , , , , , , , , , , , , , , ,	TOU



	天珣单点登录的两种登录方式	18.3
	.1 帐号/密码单点登录	18. 3
	.2 UKey 单点登录	18. 3
社证	配置利用智能卡进行 WINDOWS 身	18.4



# 1. 体系结构

# **1.1.** 中心服务器、本地服务器、客户端、以及策略网关的体系结构



# 1.2. 系统中的角色及术语

1.2.1. 角色

"中心服务器 (Center Server)":所有策略规则集中存放的地方,系统中唯一开放了配置用户界面的服务器。管理员从 Web 登录到中心服务器,进行策略配置,报表查询。本地服务器与中心服务器进行策略规则同步,报表同步。

■ "本地服务器(Local Server)":本地服务器是客户端(CC)



日常取规则的地方,也是 CC 发送报表的目的地。本地服务器从 中心服务器同步得到策略。

- 下载服务器:下载服务器是供客户下载各种运行软件,Windows Service Pack,HotFix,防病毒码以及策略系统本身的安装程序 的 Web 服务器,下载服务器可以由策略服务器兼作,也可以是 单独的服务器。
- "客户端(CC)":安装在每个被策略管理的用户的电脑上的代 理程序。执行策略的检查,从本地服务器上取规则,向本地服 务器发送报表,当用户不满足策略规则时,向用户提示相关信 息。
- "策略网关代理(PluginProxy)":管理所有关联的策略网关, 策略网关代理从本地服务器上取插件规则。当策略网关激活时, 策略网关代理将规则发送给各个关联的策略网关。策略网关代 理的主要作用在于可以将安装在多个应用服务器上的有相同规则的策略网关交给同一个策略网关代理管理,从而简化管理员的配置;同时,各个策略网关可相互共享CC的状态,如CC1在 策略网关1上通过了认证,那么通过策略网关2访问时就无需 第2次认证,提高系统性能。
- IIS 策略网关、ISA 策略网关、Exchange 策略网关以及中性(通用)策略网关:策略检查点,与 CC 配合强制用户满足策略规则。
   策略网关从所属的策略网关代理上取规则。

## 1.2.2. 术语

■ **管理网段:管理网段**是一个大的网段范围,一个管理网段可以 包含多个 IP 组。一个本地服务器可以为多个管理网段服务,每



一个**管理网段**可以由不同的管理员管理。(在当前的版本中,管 理员可以管理**本地服务器**上的所有**管理网段**)。一个**管理网段**通 常是一个园区网的地址范围。

■ **IP 组: IP 组**是设置规则的最小单位,一个管理网段划分为多个 IP 组使配置管理更加灵活。一个主机也可以配置成一个 IP 组。

## 2. WEB 控制台登录

## **2.1.** 关于 WEB 控制台登录

- 天珣支持两种登录认证模式: "Windows 集成认证登录"和"三 权分立认证登录"。在中心服务器安装时可选。在中心服务器 上登录时可输入 <u>http://localhost:8833</u>,在其他终端上登录 时则输入 http://服务器 IP:8833。
- "帐号管理员":天珣系统的帐号创建者,三权分立模式下独有,默认为:administrator,只有使用帐号管理员才能创建系统操作员和其他帐号管理员。

**注意**: Windows 集成模式下 administrator 的默认密码是中心服务器 administrator 的密码,该密码不能为空,同时该管理员登录名称不能更改,如用户环境有更改,需要重新创建 administrator 帐号和密码。

- "系统操作员":策略配置的制定者,三权分立模式下独有, 只能由帐号管理员创建。
- "系统审计员":只能对告警及审计信息进行查询的管理员,
   三权分立模式下独有,无法进行策略配置。默认帐号为



auditor,可使用这个帐号登录再创建其他系统审计员。

"系统管理员":默认与windows的administrator帐号集成, windows集成认证模式下独有。可进行策略配置,也可进行帐 号管理。

## **2.2.** Windows 集成认证登录页面

## 2.2.1. 配置介绍

此种认证登录模式与安装天珣中心服务器的 windows 的系统帐号 集成,第一次登录时默认以 "administrator" 帐号登录,密码为 系统设置的密码。若系统中没有 "administrator" 帐号,请重新 设置一个 "administrator" 帐号,使用此帐号登录一次 WEB 控制 台后再新建其他与系统帐号同名的帐号。

连接到 192.168.1.1	82	? ×
	T	
正在连接到 192.16	8.1.182 <b>.</b>	
用户名(U):	<b>2</b>	<b>•</b>
密码(E):		
	🔲 记住我的密码 🗷	
	确定	取消

## 2.2.2. 配置要点

- 1. 安装完成后,使用 "administrator" 帐号登录 WEB 界面;
- 点击"管理员设置"中的"管理员"页面,创建一个系统管理员 stra,点击"保存";
- 3. 在 windows 系统中创建一个用户 stra,此时即可使用 stra 帐



号登录天珣 WEB 管理界面进行策略配置。

**注意**:使用 windows 集成认证登录后直接进入天珣策略配置界面。 具体帐号配置操作请参考"基本配置"-"系统管理员"。

# 2.3. 三权分立认证登录页面

## 2.3.1. 配置介绍

"三权分立模式"即帐号管理员,系统操作员及系统审计员三种管理权限。此种认证登录模式使用 administrator 和 auditor 为默认帐号,默认密码为 12345678。



使用 administrator 帐号登录后界面为管理员帐号创建界面

**	3081412838.20	tions Arrest	esse.			1.00720
OWNER	******	系统酵素员	未钱粮作资献			
14050		an				
CIT N/W	· · · · · · · · · · · · · · · · · · ·		TRA18	1000	1000	-0114
	1					

在此界面中可以根据需要创建其他的帐号管理员及系统操作员,只 有在创建了一个系统操作员之后,使用系统操作员登录才能正常进 入策略配置界面。



CHRIAN CHRIST							00011.00	-0.01.00000.		
10294	53855	[88]								
	· · · · · · · · · · · · · · · · · · ·	*****	11.1.1	10000		STREET, STREET	1011.0	CONTRACTOR OF STREET,		
	af	147					2016	· •		e
	24	34				1.8	8004	.e.		
		100					Rades			
	Longing	linibes			4	4	21099		4	
	Bagnare	Taipment.					mailer			0
	CARDUNES!						12121		4	5
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	and a		× .						

## 系统操作员

点击"系统操作员"菜单,并点击"添加",进入系统操作员创建

```
界面
```

帐号管理员 <u>果统操作员</u>	复筑操作员组
系统操作员	
果皖操作员名称·	*
系统操作员全名:	*
系统操作员密码:	*
诸重复系统操作员密码。	*
是否激活:	⑦ 쟘 @ 是
是否是只读权限:	◎ 否心 是
是否全局管理员:	● 否 <sup>(1)</sup> 是
是否按需支援管理员端:	🗇 吾 🖲 是 👘 🔲 仅按需支援管理员端,不能登录Web管理界面
资产管理权限:	◎ 无 ◎ 只读 ◎ 充全控制 □ 只能管理资产
分区解扰:	◎ 不能 ● 能
<ul> <li>菜単板</li> <li>ダダ 英本記量</li> <li>ダダ 英本記量</li> <li>ダダ 美山</li> <li>マダ 市</li> <li>マダ ロ</li> <li>マダ ロ<td></td></li></ul>	
所属果统操作员逞。 注:右边有*号的项目必须输入	xin -> (-

创建系统操作员时通过选项给其分配相应的权限。

#### 帐号管理员

在此界面中可创建登录帐号,其作用与默认的 administrator 帐号相同。

### 系统操作员组

在此界面中可建立操作员组,通过对不同系统操作员分配不同的管 理网段来达到分级管理的目的。



## 系统审计员

使用 auditor 帐号登录后界面为系统审计员界面

7 Jen	<b>启明星辰</b> <sup>®</sup>	★ 天均内网安全风险管理与审计系统 <sup>重示素。 softral</sup> 章 歌: ····································
ST. CSINGUESS	Mante Storad 170300	
oversessa negre erses	系统审计员 🎫	-
	Albertish Albertish 2000 T	а длуга волоскуювания мост

在此界面中可以新建其他审计员帐号。

## 2.3.2. 配置要点

- 1. 使用 "administrator" 帐号登录天珣 WEB 控制台;
- 点击"管理员设置"中的"系统操作员"菜单,创建一个系统 操作员 strb,点击"保存";
- 3. 使用 strb 帐号登录天珣 WEB 管理界面,此时可进行策略配置;
- 4. 使用 auditor 帐号登录天珣 WEB 控制台;
- 点击"系统审计员设置"中的"系统审计员"菜单,创建一个 系统审计员 strc,点击"保存";
- 6. 使用 strc 帐号登录天珣 WEB 管理界面,此时可进行审计查询。

注意:有审计权限的全局系统操作员也是可以在策略配置界面中看 到这些审计信息。而审计员可查看到系统操作员的操作日志,系统 操作员也可查看到审计员的操作日志,但均无法查看自身的操作日 志,方便各类型管理员之间进行相互监督。



# 3. 首页

■ 在中心服务器上打开浏览器,输入<u>http://localhost:8833/</u>, 或在其他机器上输入 http://服务器 IP:8833/,然后输入用户 密码。首页显示如下内容:



**注意**:每次点击进入首页或刷新该页面时均可触发终端实时统计, 而告警数量则是一天更新一次。若一天中此页面未打开或刷新过, 则程序内部在晚上自动执行一次与数据库的同步。

- 终端数量实时统计:是服务器(包括本地服务器)管理的所有 终端数目统计的报表,可以从中查看终端总数、受控/非受控 终端,受控终端中合规及不合规的终端数量。
- 告警数量:是攻击告警统计的报表,横坐标为日期,竖坐标为告警的次数。可以查看到最近一周的安全状态,比如哪天受到的攻击最多,最近安全状况呈上升、下降还是稳定状况等等。
- 系统组件运行状态:监控各个管理服务器的性能状况和组件状态,同时也可在此界面中直接停止或重启各组件的服务。



# 4. 基本配置

## 4.1. 关于基本配置

在配置所有的策略之前,您应该先配置策略服务器、管理网段和 IP 组。在您安装中心服务器时,系统已经自动为您配置了一个中心服务器和一个初始的管理网段。在最简单的情况下,您只需再配置一个 IP 组就可以了, IP 组是策略下发和执行的最小单位。下图是策略服务器、管理网段、IP 组、网段、IP 地址关系示意图。在本系统的术语中, IP 组和网段是等同的。



## 名词解释:

- "按需支援操作员":三权分立模式下特有,建立系统操作员的同时会建立相同的一个按需支援操作员。
- "系统管理员":Windows 集成认证模式下特有,默认帐号为 administrator,密码与安装天珣服务器的那台服务器的 Windows 系统下的 administrator 密码相同。



- "策略服务器":策略服务器包括中心服务器及本地服务器, 客户端都需要连接到策略服务器来取策略。
- "管理网段":管理网段是策略能够应用的最大的网段范围, 也是系统操作员管理权限划分的基本单位。通过添加管理网段,来建立各个策略服务器管理的终端的范围,每个服务器可以管理一个或多个管理网段,只有在管理网段范围里的终端才能根据后续的 IP 组设置来确定是否能从这台策略服务器中拿取策略。
- "IP 组": IP 组是系统管理的最小的 IP 策略应用对象单元。
   IP 组是管理网段下的子网段或单独的 IP 地址,一个 IP 组可
   包含多个网段或独立 IP 地址。
- "部门":添加部门信息,对上报的终端划分部门类别,客户端在注册时即可自己填写相应的部门,在进行报表查询时可通过选择部门来丰富展现的形式。
- "终端注册":可以在页面上修改已注册终端的部门信息,或
   者通过管理员手工的方式来注册未注册的客户端。
- "本地用户":本地用户是天珣自带的一种目录服务。本地用 户就是用来存储用户信息在服务器本地中,为用户认证或者证 书认证提供查找认证信息服务。
- "用户组":用户逻辑组是基于用户设置策略的最小的用户策
   略应用对象单元。用户逻辑组可以包含 LDAP 中的 Group 和
   用户还有本地用户。
- "可信 MAC":管理员可以预先设定的终端 MAC 地址列表, 在其中列出的 MAC 称之为可信 MAC。可信 MAC 可以作为一 项认证条件,与准入控制或安全控制结合对客户端进行合法性 认证。
- "可信 GUID":管理员可以预先设定的终端 GUID 列表,在 其中列出的 GUID 称之为可信 GUID。可信 GUID 可以作为一 项认证条件,与准入控制或安全控制结合对客户端进行合法性 认证。



- "用户、IP、MAC组合":管理员可以预先设置用户、IP、 MAC的组合关系列表,并可作为一项认证条件,与准入控制 或安全控制结合对客户端进行合法性认证。
- "网络设备配置": 启用准入控制的网络设备的配置,同时可以添加端口绑定,将端口作为一项认证条件,,与准入控制或安全控制结合对客户端进行合法性认证。
- "分组信息":已安装客户端的终端并上报了报表信息后,将
   终端的工作组信息分组展现。
- "**全局参数"**:所有客户端和服务器的全局基本配置参数。

## 4.2. 按需支援操作员

## 4.2.1. 配置介绍

此菜单为三权分立模式下特有,在帐号管理员建立系统操作员时, 若选择其同时是按需支援操作员的话,在此处将会出现一个同名的 按需支援操作员。在系统操作员登录时将无法修改此处的配置。

技需支援操作员	35.30			64
<b>我面交话操作员</b>	輸作符会名	息亦曲抗	的改变的	-
and the second s	art	*		
10.	jek	4	1	
ling	jing	4	1	
liurithing	liwithing	A	1	
ningris linguis	alagrasjinggas	A	2	
mine	yyhop		2	

点击"**添加**",进入"**添加按需支援操作员**",可用于添加只有按需 支援功能的操作员。



技需支援操作员			
按整文規操作员名称:	8	-	<u>租助</u>
按齋支銀操作员全名:	-		
按量支援操作员密码:		-	
请重复按需文据操作员密码:			
是否教话:	02.00		

配置项:	<u>说明</u>
按需支援操作员名称	按需支援操作员的登录 ID
按需支援操作员全名	按需支援操作员全名
按需支援操作员密码	输入对应的密码
请重复按需支援操作员密 码	重复输入对应的密码
是否激活	如果不激活,则该管理员将无法登录按 需支援管理界面

创建完成后可点击笔形按钮修改密码。

## 4.2.2. 配置要点

- 1、 点击"添加"按钮, 输入"按需支援操作员名称" jch1
- 2、输入"按需支援操作员全名"jch1
- 3、输入"按需支援操作员密码",并输入"请重复按需支援操作员密码"
- 4、点击"保存"

# 4.3. 系统管理员

## 4.3.1. 配置介绍

此菜单为 windows 集成认证模式下特有。可在此菜单下添加除 administrator 外的其他系统管理员,并可在管理员组中根据不同的 管理网段分配不同权限给非全局管理员。



AREA TER TERE

系统管理员	33							
10248	TELES	8686	4614	10121	SQUEEDA	8.198	BARETE	1078-5
shinoveter	1155		E.		4	8128	4	
atte	非经审计合	4		4		72.51	8	

## 添加管理员

点击 <b>"添加</b> ",进入添加	П" <b>系统管理员"</b> 。	
管理员组		
系统管理员		
管理员名称		
管理员全名	· · ·	
是否微括	の茶の湯	
是否是只读初限	の否に是	
是否全局管理员	ゆるの是	
是否按需支援管理员端	○ 否 @ 是 □ 収接需支	援管理员端,不能登录Web管理界面
资产管理权限	○ 无 ○ 只读 ◎ 完全控制	□ 只能管理资产
分区解扰	○ 不能 ☞ 能	
- 菜单授权		
● ▼ 基本配置		
➡ ☑ 安全基线		
● 12 進入控制		т
➡ 🔽 安全防护		1
● ₩ 补丁管理		
➡ ₩ 非法外联		
母 ▼ 移动存储		
➡ ☑ 终端审计		

配置项:	<u>说明</u>
管理员名称	管理员的登录 <b>ID</b> ,必须与策略服务器操 作系统中的用户名相同。
管理员全名	与策略服务器操作系统中用户的全名对 应。
是否激活	如果不激活,则该管理员将无法登录获 得管理权限。
是否是只读权限	如果选择"只读权限",则该管理员只能查 看其所管理的服务器的配置信息,不能 修改。
是否全局管理员	如果管理员为全局管理员,则该管理员 具有最大的权限,能查看,修改,删除 任何管理员所做的配置。
是否按需支援管理员端	如果管理员为按需支援管理员,则该管 理员可为用户提供远程桌面援助。按需



	支援管理员需要安装按需支援监控端程 序 hodviewer,监听客户端发起的远程 桌面帮助请求。
资产管理权限	设定管理员对资产模块的管理权限,有 只读、完全控制和只能管理资产三种。 只读权限只能查看资产信息;完全控制 权限可进行查看、修改、删除等操作; 只能管理资产权限表示登录 WEB 控制台 时,只能管理资产信息,不能查看编辑 其他策略。
分区解扰	授权该用户是否有解扰分区加扰后的移 动存储设备的权限
菜单授权	对管理能访问的菜单进行授权
所属管理员组	一个管理员可以属于多个管理员组,不同的管理员组管理不同的策略服务器,因而一个管理员可以管理多个策略服务器。

#### 添加管理员组

天珣内网安全风险管理与审计系统以 IP 组为权限管理的单位。不同的管理员组管理不同的管理网段,一个管理员可以同时属于多个组,因而一个管理员可以管理多个管理网段。点击"管理员组"设置,系统显示所有现存的组。

#### 点击"添加",进入添加管理员组

#### 管理员组

组名称	组(192.168.1.1/24) *
組描述	此管理员组的用户具有管理 🗾 192.168.1.X/24网段的权限
是否激活	○否
所管理的管理网段	初始管理网段 NAT管理网段(100) <- 192.168.1.*
注:右边有*号的项目必须输	俞入。
	保存 圖除 取消
配置项:	<u>说明</u>



组名称	请输入便于记忆的管理员组名称。
组描述	请输入关于这个管理员组的额外信息。
是否激活	如果不激活,则从属于此组的管理员将 无法管理组内的服务器。主要用于测试 方便,建议使用默认值。
所管理的管理网段	管理员组可管理一个或多个管理网段, 左边的列表是系统中所有的管理网段, 右边的列表是该管理员组所管理的管 理网段。

**注意**:当属于某一管理员组的非全局管理员帐号登录时,其所得到的权限仅限于其管理员组所管理的网段,无法对所有不属于此网段的 IP 组进行策略配置。

## 4.3.2. 配置要点

**配置前提:**新增一个新的管理员时,必须确保 windows 系统中有相同名称的用户,且该用户的密码不为空

- 以系统管理员登录 Web 控制台,点击"管理员组"中的"添加"按 钮,输入"组名称"test1,点击"->"号将"所管理的管理网段" 列表中的 miprange1 网段移动到右列中,点击"保存"。
- 2. 点击"管理员"中的"添加"按钮,输入"管理员名称"testadmin1, "管理员全名"testadmin1,"是否激活"选"是","是否只读权限"选"否","是否全局管理员"选"否","是否按需支援管理员端"选"是","资产管理权限"选"完全控制","分区解扰"选"能", 点击"->"将"所属管理员组"中的test1移动到右列中,点击"保存"。
- 3. 使用 testadmin1 帐号登录 WEB 管理控制台,此帐号拥有全部策略 配置权限,但只能对 miprange1 网段所管理的 IP 组生效。



# 4.4. 策略服务器

## 4.4.1. 配置介绍

点击"策略服务器"选项,显示系统中所有的服务器,用户可以添加新的服务器,编辑,删除现有的服务器。

策略服务器					
策略服务器	添加				
服务器名称	IP地址	中心服务器IP地址	是否激活	管理端口	资产管理
224的本地服务器	192.168.0.224	192. 168. 1. 16	是	8833	启用
CenterServer	192.168.1.16	192. 168. 1. 16	是	8833	启用

#### 添加服务器

点击"添加"进入添加服务器

<u>策略服务器</u>	
策略服务器	
服务器名称	CenterServer *
服务器描述	中心服务器
IP地址	192.168.1.10 *格式如:10.156.100.18
中心服务器IP地址	192.168.1.10 *
使用中心服务器的数据库连接参数	●是 ●否
SQL Server数据库连接参数	检查数据库连接
数据库服务器IP地址	192. 168. 1. 10
端口	1433
用户名	tx_user
密码	••••••
注:右边有*号的项目必须输入。	
	保存取消

配置项:	说明
服务器名称	请输入便于识别的服务器名称
服务器描述	请输入此服务器的额外信息,方便管理



IP 地址	安装本策略服务器的电脑的 IP 地址		
中心服务器 IP 地址	安装有中心策略服务器的电脑的 IP 地址。如果本策略服务器就是中心服务器,请填自己的 IP 地址。		
使用中心服务器的数据 库连接参数	在添加本地服务器时,可选择此项,如 果选择"是",则直接使用与中心服务器 相同的数据库,如果选择"否",则需要 配置下面的数据库连接选项		
数据库服务器 IP 地址	输入本地服务器所使用的数据库 IP 地址		
端口	输入本地服务器所使用的数据库端口地 址,默认为1433		
用户名	输入数据库连接用户名		
密码	输入数据库连接密码		

注意:

- ◆ 天珣使用的登录 WEB 服务器的管理端口为 8833, 此端口不可 修改。
- 资产服务器在中心服务器安装时默认已和中心服务器一起安装,因此无需单独安装。
- 在添加本地服务器时必须指定正确的中心服务器 IP 地址,否则该服务器不能与中心服务器同步,因而不能得到最新的策略规则,同时也会影响该服务器所管理的 CC,当 CC 的 Primary Server 和 Secondary Server 都不可用时,中心服务器是 CC 取规则的策略服务器。



# 4.5. 管理网段

## 4.5.1. 配置介绍

点击管理网段的页面标签,将显示管理员设置的所有服务器的管理 网段,通过所属主服务器的不同来区别是中心服务器还是本地服务 器的管理网段。

通过添加管理网段,来建立各个策略服务器管理的终端的范围,每 个服务器可以管理一个或多个网段,只有在管理网段范围里的终端 才能根据后续的 IP 组设置来确定是否能从这台策略服务器中拿取 策略。

#### 添加管理网段

点击"管理网段"页面上的"添加"按钮进入添加管理网段界面。

管理网段		
管理网段名称	172	,
管理网段描述		
		-
管理网段开始IP地址	172.25.0.1	
管理网段结束IP地址	172. 25. 255. 255	,
Primary Server	CenterServer	• *
Secondary Server	CenterServer	•,
是否使用默认的下载服务器	0 否 ●是	
下载服务器地址		
停止客户端服务程序时是否需要验证密码	0 否 0 是	
卸載客戶端时是否需要验证密码	○否會是	
客户端卸载及停止服务密码	•••••	显示明文
注:右边有*号的项目必须输入。	保在删除取消	

管理网段名称

您能记得住的名称。



管理网段描述	您可以输入关于这个网段的额外信息。
管理网段开始 IP 地址	网段不一定是完整的 B 类、C 类或其它完整的子网,可以从任何一个地址开始。
管理网段结束 IP 地址	这个地址也是任意的,但应该大于开始的 IP 地址。注意不同的管理网段的 IP 地址不 要有重叠。
Primary Server	本管理网段的主策略服务器。每个网段的 客户端首先从主策略服务器取策略,如果 失败,则从辅策略服务器取策略,如果失 败,则从中心服务器取策略。
Secondary Server	本管理网段的辅策略服务器。
是否使用默认的下载 服务器	如果选择"是",则下面的"下载服务器地 址"不可填,系统将使用 http://策略服务器 IP:8833/download/作为下载服务器地址。如 果选择"否",将使用"下载服务器地址" 输入的 URL 作为下载服务器地址。
下载服务器地址	下载服务器供客户端下载红名单中的软件、防病毒软件升级码,补丁程序等。默认的下载服务器地址为http://策略服务器 IP:8833/download/。如果您使用其他的下载服务器,请在此处输入该服务器的URL地址。红名单软件、防病毒软件升级码、补丁程序等的下载URL只需输入"下载服务器地址"后面的相对路径部分。比如一个红名单软件的下载地址为http://策略服务器IP:8833/download/software/abc.exe,那么,红名单配置中的"下载URL"只需填



	写"software/abc.exe"。	
停止客户端服务程序 时是否需要验证密码	设置停止客户端服务时是否需要输入密码	
卸载客户端时是否需 要验证密码	设置卸载客户端时是否需要输入密码	
客户端卸载及停止服 务密码	设置卸载及停止服务的密码	

一个管理网段中配置的 IP 地址段可以是整个子网,比如
"192.168.0.1-192.168.1.255",也可以是一小段连续的 IP,比如
"192.168.0.40-192.168.0.50",但无法配置为单个 IP 地址。

注意:删除某个管理网段时,将同时删除这个管理网段下建立的所有 IP 组,并且对这些 IP 组生效的策略也将失效(若这些策略关联 了其他 IP 组,将不会受影响)。

## 4.5.2. 配置要点

- 1. 点击"添加"按钮,进入添加"管理网段"界面
- 2. 输入"管理网段名称"为本地服务器网段
- 3. 输入"管理网段开始 IP 地址" 192.168.1.1
- 4. 输入"管理网段结束 IP 地址" 192. 168. 1. 254
- 5. 选择 "Primary Server" 为本地服务器
- 6. 选择"Secondary Server"为CenterServer
- 7. 点击"保存"
- 8. 此时已为本地服务器定义了管理网段为 192.168.1.1-192.168.1.254范围,所有这个网段下的客户端 均将通过本地服务器连接拿取策略。



# **4.6.** IP 组

## 4.6.1. 配置介绍

IP 组是设置策略的最小单位,一个管理网段划分为多个 IP 组使配置管理更加灵活,一个主机也可以配置成一个 IP 组。

一台终端的 IP 地址必须属于设定的某个 IP 组才能正常获取到此 IP 组的策略,而这个 IP 组必须属于某个管理网段所管理。

#### IP 组

点击"IP 组"标签,默认将显示所有服务器的所有管理网段下已 建立的所有 IP 组。

<u>IP组</u> 工作时间			
IP组 查询IP组 所有管理网段	m ▼ 只显示包含指定地址的組		拉条件查询IP组
			<u>帮助</u>
IP组名称	所屬管理阿段	内容	
test	初始管理网段	192.168.1.1-192.168.1.254;	
1			

通过页面上的查询 IP 组条件,可以分别对某个或某些 IP 组进行查询。

按条件查询IP组

点击管理网段的下拉菜单,可以选择配置好的管理网段;选择好查 询条件后,点击"按条件查询 IP 组"按钮,将查询出相应的 IP 组。

IPill AN		Sin	
「MTURZ 163, 110, 0+」 円載示包含案 当前主義: 吉徳円記 AFTUR 10: 110 0	5832498 941	投資作充潮計算	
0888	N3014-5-2	AUTHAS	
NAT 1740 (182 108 100 1021)	Contention or	N7192 180 180 07240	MT 2100 ( 100, 100, 111, 0/24)

如果知道某台客户端的 IP 地址,想查询其所属的 IP 组,那么只需 要在"**只显示包含指定地址的组**"中输入此 IP 地址,然后点击"按



条件查询 IP 组"按钮,即可查询出其所属的 IP 组信息。

点击"添加"按钮进入 IP 组设置界面

11 100-02 40	test			
田植物注	1			
所屬的服务器	CenterServer			
所属的世界问题	初始管理构段			
本IP组中的IP地址	58	开始地址	粘水地址	
				海流
	152, 168, 1	192 168 1 1	192 168 1 254	1 8
网络的地址	12	1746.92	- 5	-
	1			漢加
工作时间	不说豐工作时间。	3		
本12/组应用的策略	<u>***</u> 844	<del></del>		
UERS				
	不 不 名用			
暴苦启用用户以证				
鼻舌包用用户以证	日用			
暴苦包用用户以证 选择包用的目录服务	「 <b>日用</b> 「「 半地用户			
最著名用用户以近 法指包用約日本服务 用户、II、 MC相会以正	「日用 同学地用戸 『不倉用			

配置项:	说明
IP 组名称	您能记住的 IP 组名称
IP 组描述	您可以输入关于这个 IP 组的描述信息。
所属的服务器	选择这个 IP 组是被哪个策略服务器管理。这个 服务器是 IP 组所在管理网段的主策略服务器 (Primary Server)。
所属的管理网段	选择这个 IP 组属于哪个管理网段。这个选项的 内容会根据"所属的服务器"的内容变化,如 果改变"所属的服务器",则"所属的管理网 段"只出现选择的服务器所管理的管理网段。
排除的地址	IP 组可以包含一个或多个网段,可以对网段中



	的某些 IP 地址进行排除。IP 地址被排除后,
	这个 IP 地址将不获取策略,系统的应用准入机
	制也不对这个 IP 地址进行强制策略检查。如果
	这个排除的 IP 地址在另一个 IP 组中以独立 IP
	存在,那么这个 IP 地址对应的策略以那个 IP
	组的策略为准。
	输入 IP 组名称和具体的 IP 地址范围并添加来
本 IP 组中的 IP 地	定义此 IP 组。添加后可通过笔形按钮进行修
址	改,也可通过 X 形按钮进行删除。
	选择工作时间选项,工作时间策略的订制可在
工作时间	" <b>工作时间"</b> 菜单中添加
	通过查看及编辑按钮进行此 IP 组的相应策略
本 IP 组应用的策	配置。若此 IP 组还没有设置策略的话,则会在
略	此处提示用户 <b>"还没有应用策略"</b> 。
	在非网络准入的前提下进行的认证选项,可以
	和"可信 MAC"、"用户、MAC、IP"组合成完善
	的认证模式。基本认证包括三个选项:不启用
认证策略	时客户端无需进行认证,"仅客户端运行"接
	入电脑只需运行了客户端即可通过验证。"用
	<b>户认证"</b> 不但需要验证客户端运行,而且需要
	与第三方认证系统连接,验证用户的有效性。
	启用用户认证后,需要选择一个目录服务的认
	证系统,这个目录服务需要在"用户组"中建
来这中田的日子明	立。通过这个第三方的认证系统,比如 AD 域,
远洋后用的日求服	客户端需要进行用户密码的认证,只有输入符
77	合 AD 域中的用户和密码才能正常认证。选择其
	中一个目录服务时,在其前面的方框内打勾即
	可。同时也可选择进行本地用户认证。



	通过用户、IP、MAC 三种条件对客户端进行组
	合绑定认证。可进行 MAC-IP 和 USER-MAC-IP
	认证。在验证输入的用户认证是正确的基础上,
	再对客户端的 IP 和 MAC 地址进行唯一性认证。
	在客户端输入用户名和密码后,将对其 MAC 和
	IP 进行校验,只有符合这个组合认证里的 IP
	和 MAC 才能正常完成认证,否则将会提示客户
组合认证	端不符合安全规范; MAC-IP 组合认证时, 客户
	端无需输入用户名密码,只对本机 MAC 和 IP
	进行验证,若 MAC 与 IP 不符合绑定策略的话,
	将认证不成功,提示客户端不符合安全规范。
	组合策略需要在"用户、IP、MAC 组合"页面
	中进行配置。
	对接入认证的机器进行 MAC 地址的检查,属于
	可信 MAC 范围的将会认证成功,否则将被认为
可信 MAC 认让	不符合安全规范。策略需要在"可信 MAC"页
	面中进行配置。

**注意**:在已定义的工作时间范围内的终端将会显示为在线,非工作时间范围的终端将会显示为离线,并启用离线策略。

**注意**:此处添加的 IP 组地址范围必须与其管理网段范围一致,否则无法正常保存。

点击本 IP 组应用的策略的"**查看及编辑**"按钮,进入应用策略的 编辑界面



IP組		一個	
ip 194 应用的策■	6 <b></b>		
2284			948
Ribr			
12 <b>50</b> 72			-
<b>#1224</b>			SVEL.
加速率计	()](第1年7		
1111年1	grist access		
89988 <b>8</b>			
1000			66

在此界面中会显示已经应用到此 IP 组的策略的列表,要将策略加入此 IP 组,请点击相应模块的"编辑"按钮,进入策略选择界面

IP组	
IP组	新助
ip 194 应用的策略	
审计策略 <b>全部收起</b> □ <b>文件审计</b>	
□ 审计共享目录 □ 审计网络拷贝	
<ul> <li>□ 审计所有本地盘</li> <li>□ 审计所有移动盘</li> <li>□ WRL审计</li> </ul>	
✓ UBL审计了 目打印审计(只能选一个黑色策略或一个绿色策略加一个红色策略)	
☞ print access 展存 取 通	

在此界面中会列出己配置的所有对应此模块的策略,需要将某条策略加入此 IP 组,只需在这条策略前勾选后保存即可。

**注意**:策略必须事先编辑好,也可在编辑好策略后,在策略配置界 面里直接将 IP 组加入。

### 工作时间

通过设定工作时间来定义用户上下班时间,在工作时间范围内即为 上班时间,终端使用在线策略,而在工作时间范围外时即视为下班 时间,终端使用离线策略。



IPM IRMN			
工作时间设置			
工作的考虑称			
工作日	周一 「周二 「周三 「周四 「周五 「周六 「周白		
Tanta .	新聞の 新聞の 新聞の 新聞の 新聞の 新聞の 新聞の 新聞の		
加旺日期及时间	开始时间 地址时间  时间段名称 开始时间 税业时间  何2010-5-25.9:00 例2010-5-25.13:30 解戦 国際		
休暇日期及时间	17月2日月前 私営(1月前) 17月1日日 - 17月2日 - 17月2日 - 17月2日 - 17月1日 1月1日日 - 17月2日 - 17月1日 - 17月11日 - 1711000000000000000000000000000000000		
往:右边有+号的项目必须输入 [個	在 後前		
配置项:	说明		
工作时间名称	输入策略名称		
工作口	选择工作时间为几个工作日,通过勾选即可实		
	现		
工作时间	添加工作时间段,直接输入时间点如9:00		
加班日期及时间	添加加班日期和时间段		
休假日期及时间	添加休假日期和时间段		

配置完成后,需在 IP 组配置中应用已经配置好的时间段策略。

# 4.7. 部门

## 4.7.1. 配置介绍

通过设置各级部门来对客户端进行部门划分,使其在客户端注册时 可以自由选择自己所在的部门,并在报表中体现出不同部门的展现 需求。 **部门**


* 13	地系铁器在员都们关联	
部门	[加重的译[]	
		<u>R8</u>
a STREET	a Cikit	\$17.8.8T)
gebent.		使和注意到门
-develop	nest.	这地下引起IT
- (12)-1		(INTER)
-8.	人力資源課	适加下积留(1)

点击"**添加顶级部门"**对部门进行添加

部门 本地系统操作员部门	关联	
部门		
上級部门	没有上级部门	
部门名称	市场部 *	к
部门描述	*	
	Ψ.	
注:右边有*号的项目必须输入。	保存 取消	

点击"添加下级部门"对这个顶级部门进行下级部门的设置

部门 本地系统操作员部门	关 <del>联</del>
部门	
上级部门	市场部
部门名称	*
部门描述	
	~
注: 右边有*号的项目必须输入。	保存 取消

### 调整部门树层次

在创建了很多部门后,如果想将一些部门调整到比较显眼的位置,或 者是将比较重要的部门调整到前排,则可以使用部门树右边的上下 箭头进行调整,既可以选择上调一级,下调一级;也可以选择置顶或 者直接调到最后一行。

部门 科理教部门		
		帮助
日和	新闻推进	和時间
金中国		(後部)
主要を中心		
		$\cup$



注意: 部门前后顺序调整只支持同级部门之间的前后顺序调整。

### 本地系统操作员部门关联

在创建了非全局管理系统操作员之后,使用全局管理员登录管理界 面时可以在这个页面看到所有创建的非全局管理系统操作员,并可 对其赋予管理个别部门的权限,有此权限的系统操作员即可查看其 管理的部门的报表等信息。

部门 本地系統操作员部门关联			
1 (1 5)(소비나다 20)가 11 8일			
本地糸统操作员部门天联			-
			<u>帮助</u>
系統操作员名称	系统操作员全名	所管理的部门	
<u>44</u>	444	testi	
m	777	support;	

点击系统操作员名称链接,进入后对其进行部门权限的分配

```
部门 本地系统操作员部门关联
```

#### 本地系统操作员部门关联

系统操作员名称	44
系统操作员全名	444
所属部门	■.部门管理 

勾选相应部门后点击"保存"即可。

# 4.8. 终端注册

## 4.8.1. 配置介绍

配置完部门后,可在客户端全局参数处启用客户端注册功能,启用 注册功能后就能通过终端注册的管理来查看或修改已注册客户端 信息,或者页面上手工完成未注册客户端的信息填写。

### 开启客户端注册功能





》 國页 言 - 9基本政告	试用版授权。2012年2月1日到期1 <u> 森介紹介ி等数</u> 服务器全局等数	Y.				
<ul> <li>・付着支援時件内</li> <li>・分割(用力)</li> <li>・分割(用力)</li> <li>・分割(用力)</li> <li>・分割(用)</li> <li>・分割(用)</li></ul>	客户端注册参数 毕还自用客户编主册 时以下已期前主册的客户课- 美术重新主册 客户编主册重复是示调明		1970-1-1 0	E3		
- D 印值WAC - O 印值GOD	tractorit		(0美示不整算提示。)			
ORIP.MARCER	and a dealer of	171	211 CONTRACTOR	Contraction of the local division of the loc	and the local division of	- 240
DyBon	ini T		12			
や安全基成	使用人					
中違入控制 由中心的助	Intel I	11	1	14		
0)计丁管理	地址	21	385	t 4		
の波戸管理	电线	15	100	0 4		
0份站存储 0把建审计			保存 政府	( howkees		

在上页面上,管理员还可以增加自己想要的注册项目。

### 终端手工注册

使用终端手工注册来给客户端进行注册,若已启用进行客户端注册 的策略配置,而用户因为疏忽或不想注册的话,则可以在此处由管 理员对其进行手工注册,将客户端与部门进行绑定。

冬靖手工往 册			
1.91.44	#mer	ig War	10.00 4110
· RACREM	17.98.92	F47-9254	186
E BORNASTAN	172 15 122 190	172 25 122 +4	LINC-0753
00-0-20-20-0-01-00	172.29.90.19	172.25.96.19	400H-PC
10-0-21-08-00-0T	192 349 1.190	192, 169, 1, 196	TRETAURE-Se
E 00.9+0+1+17:4	172 35 99 99	172.25.06.99	754899-00921488
E 00-20 18-01-40-44	172, 25, 90, 198	172.25.90.100	RECOLDINE:
00-0-28-20-W-Th	172 12 98 14	172.25.56.14	2000-002-2
E 10-0-28-00-18-18-	172.25.70.9	172, 25, 79, 9	KURUE-9482 30066
E 10-20-20-02-01-02	1982 188 1 41	192 169 1.41	AIMTH-HOTFER
11			
注册进中的传输	注册所有的焊续		

通过主机名或 IP 范围可查询出相应已受控的客户端,在方框处打 勾后点击"**注册选中的终端**"进行手工注册,也可直接点击"**注册** 所有的终端"对所有终端进行注册。

### 修改注册信息

若已启用进行客户端注册的策略配置,那么可以在此处可以查询到 正常注册的客户端提交的注册信息以及管理员手工注册的信息,管 理员可以对其进行部分调整,手工修改注册信息。



80	注量信息						
E	1.004200	a Aligan	18927			(enanwiesnaal) 🗆 Mi) 78	Transies and 1
Ď	10.00	11763	ALC: NO.	256	811	1	13. 1800
1	2010/12/16/16	107.75 79.9	18-8-91	2010 C	305	14	a 200-07-0
13	2-11-0-10-0-11	10.25 ± 23	175 25 A 221	theopete		Yes	n 201-0-1
10	0+4+0+(1-0-0	m 3 % II	12.89.0	ii wil?	independent Versignant		201-42-1

在 mac 地址前的方框中打勾,然后点击"修改选中终端的部门信息",即可修改这些选中终端的部门信息。点击"修改所有终端的部门信息",可以将所有终端部门信息修改。点击"删除选中终端 信息"即可删除选中的终端注册信息,删除之后客户端会根据策略 重新上报。点击"导出到 Excel"可以将导出已注册客户端的信息。

**注意**: 客户端注册时支持客户端处于 NAT 环境下,在上报注册信息时会将客户端真实 IP 和 NAT 后的 IP 同时报上来,方便区分。

# 4.9. 本地用户

## 4.9.1. 配置介绍

本地用户是天珣自带的一种目录服务。目录服务将有关信息存储为 具有描述性属性的对象。人们可以使用该服务按名称查找对象,可 使用它们查找服务,同时获得对应的资源或信息。本地用户就是用 来存储用户信息在服务器本地中,为用户认证或者证书认证提供查 找认证信息服务。

点击	音"本地用户"	'标签,将	F显示服务器上	现有的本地用户信	言息
2	<u> </u>				
	本地用户	添加用户	<b>令入用户</b> 导出	出用户 下载模版	
	<u>登录名</u>	<u>姓名</u>	<u>数字证书用户名</u>	修改密码	1
	EPOS	EPOS	EPOS	1	
	1				



本地用户		
雅莽石	1	<b>—</b> .
推古	Ì	<u> </u>
教学证书用户名	-	
1849	ř.	())●市場力学校正常以用户名/市場力大量●
WKA (258	ř.	
电话号码	i	
电子邮件	í -	
该:古边有+号的用目必须4	a.A.	

配置项:	说明
登录名(必填)	本地用户认证时的用户登录名
姓名(必填)	用户的姓名
数字证书用户名	证书认证时的证书名(需在用户组-目录服 务中的本地用户配置相关信息才能使用)
密码	本地用户认证时的登录密码
确认密码	再次确认登录密码
电话号码	用户的电话
电子邮件	用户的电子邮件

**注意**:登录名和证书名在本地用户中是唯一的,不能有相同的名字 出现;用户密码为空时,必须填上数字证书用户名,认证时只能用 证书认证。

"**本地用户**"标签下,点击"**导入用户**"按钮,可以批量导入事先 储存在本地某个 excel 表中的用户信息。



本地用户	添加用户	导入用户 导出用户	下载模版
<u>登录名</u>	姓名	<u>数字证书用户名</u>	條改密码
EFOS	EPOS	rpos	1
venus	EPOS	venus	1
1			

点击"**导出用户**"按钮,可以将服务器的本地用户信息导出到一个 excel 表中,此 excel 表就可以作为"导入用户"的信息表。

点击"**下载模板**"按钮,可下载一个 excel 表的用户信息模板,在 表里填入用户信息,就可以作为"导入用户"的信息表。

点击修改密码的笔型按钮,可以修改本地用户的密码。

# 4.10. 用户组

## 4.10.1. 配置介绍

本系统支持自带的本地用户认证,或者与第三方认证系统联动完成 用户认证,采用标准的 LDAP 协议,支持的第三方认证系统包括 AD 域,iPlanet,OpenLDAP 等。这些也称为"目录服务"。如果您 的网络中没有认证系统,您可以下载安装免费的 iPlanet 软件,建 立一个简单且安全的认证系统。

与 IP 组类似,本系统支持用户逻辑组。用户逻辑组是基于用户设置策略的最小的对象单元。用户逻辑组可以包含 LDAP 中的 Group 和用户。

下图是目录服务、LDAP 用户,逻辑组之间的关系图





下图是通过第三方认证服务器认证过程示意图



## 目录服务

点击"目录服务"标签,显示服务器现有的目录服务信息。

日求服务	用尸狙		
日寻昭条	添加		
ц жл <u>х</u> Э	13-134		
			<u>帮助</u>
目录服务名称		目录服务类型	
本地用户		本地用户	
<u>ad11</u>		Active Directory Server	



				READ
<b>計名称</b>	adii			
录服务路径	do=testwork, dc=con			
<b>予服务类型</b>	Active Directory Server	•		
阿用戶名	administrator			
同密码			和和	
录服务器内表			添加服务器	
	192, 168, 1, 11			
		-	验進育的顧荼書	
季度芬参数	无	-		

配置项:	<u>说明</u>
目录名称	设置您企业的目录服务的名称。



	LDAP 管理域的目录服务路径,例如域
	名为 sample.com,如果目录类型为 AD 域,则填写格式可参考:
目录服务路径	dc=sample, dc=com; 如果目录类型为
	SUN 的 iPlanet, 则填与格式可参考: OU=People, dc=sample, dc=com。
目录服务类型	本系统支持 AD、iPlanet、OpenLdap 三种目录服务类型。
访问用户名	本系统访问目录服务所用的用户,该用 户只需具有读取活动目录的权限即可。 输入用户名时建议在用户名前加上域 名 例加, samplo)administrator 在
	h, 阿如: Sample (administrator。在 iPlanet 环境中, 必须输入用户名: CN=Directory Manager。
访问密码	本系统访问目录服务所用的用户的密 码。
目录服务器列表	目录服务器列表,可通过输入目录服务 器的 IP 或域名来添加,可添加多台服 务器。
目录参数	iPlanet 和 OpenLdap 环境中,可建立 动态组,此参数用于设置刷新动态组缓 存的时间间隔,默认为 24 小时(86400 秒)。

注意:如果是 iPlanet 的话,输入的用户名必须是 CN= Directory Manager, 密码也必须是创建 iPlanet 时建立好的 Directory Manager 密码,否则将无法验证成功。

输入完服务器 IP 后,点击"访问密码"右侧的"检验"图标,可



以直接进行模拟验证,如果配置正确的话将验证成功,否则会给出 适当提示。

本系统也支持自带的 **"本地用户"**目录服务,在"**目录服务**"标签的页面下点击 "**本地用户**",进入本地用户配置页面。

目录服务					
1958	本地用户				
日录服务共和	(本規用产		9		
受保住的证书得发现构	UTHORN NONE # : [		Browse	93	
	05# 05	e (1811)	W.	2856	<b>8</b> 46
<b>亚书状态制</b> 证	件不能定证书状态 (* 先进行在根据证,表	acvilli ##################################	不可用时使用用	用正式的复数证	
证书状态验证 RABE书列表	中 不能定述系统法 「 先達内在映影正, 法 () () () () () () () () () () () () ()	arabi Abdrabi Abi Lina ang kanakari Lina ang kanakari	FREE BEER	nesymatic Contraction Mate	

配置项:	<u>说明</u>
目录名称(必填)	设置本地用户的目录服务的名称,默认
	为"本地用户"
目录服务类型	不能修改,默认为"本地用户"
受信任的证书颁发机构	导入证书颁发机构颁发的根证书,为用
	户认证时验证用户证书提供信息
	选择"不验证证书状态",则证书认证
	时不验证证书是否已被吊销, 仅需要
	认证是否是可信的 ca 颁发的.
	选择"先进行在线验证,没有 CA 服务
证书状态验证	器或 CA 服务器不可用时使用吊销证书
	<b>列表验证"</b> ,则要验证证书是否己被吊
	销,验证方式为先到 CA 服务器在线验
	证,没有 CA 服务器或 CA 服务器不可用
	时则用吊销证书列表验证,需要配置下



	面的配置项
吊销证书列表	添加一个从 CA 服务器发布的一个吊销 证书 clr 列表,验证证书是否已被吊销
在线验证 CA 服务器列表	添加在线的 CA 服务器,用于实时在线 验证证书状态是否已被吊销

## 用户组

添加完目录服务之后,我们就可以在用户组选项里设置用户组了。 用户组是系统设置用户规则的对象单位,目录服务中的用户组或用 户必须加入到这里才能被设置用户规则。一个用户可以属于多个用 户组。

点击"用户组"选项,查看已经存在的用户组列表。

HRES	MP.M		
用户组	26:38:		
THP NUMBER		Ball Mark	1
ad <u>group</u> andres anas		192.168.1.11	
3			

点击"添加"进入添加用户组配置页面

目录服务	用户组	
用户组		
		<u>帮助</u>
用户组名称	ad_group	*
描述信息	192.168.1.11	<u>A</u>
		<b>v</b>
用户组成员	查看及编辑	
应用的策略	查看及编辑	
注:右边有*号的	的项目必须输入。	
	保存 删除 取消	

配置项:	<u>说明</u>
用户组名称	您能记住的名称。
描述信息	您可以输入关于这个逻辑组的额外信

	息。
用户组成员	通过查看和编辑选项,连接域服务器添 加用户和用户组。
应用的策略	通过查看和编辑选线,对设置好的策略 进行应用。

点击用户组成员的"查看及编辑"选项,进入编辑用户组成员界面

19.93	15	MPM			
989 .A.83	电用户 4.8.53	until [************************************	8.000/28	ana Stud	Atta
		LANGE D BERN	IRNAE ID	#PLIS	filmat 0
	1.1.1		IL CARLES		ASPARK
T.	22	Administrator	stit	.4	CREAdoublishmeter, CREASers, DC-texteech, SC-com
10	22	and figs a	+411		Million of Speed, Cliff Source, Million Strategies, Chilling
馬	22	ACTRE	+#11	4	DP+G2NET, DP-liners, DC+textexck, 3C+em
E.	22	darres	adil	4	19-dames, DP-fract, DD-testwork, 30-rose
F	57	Ducit	+d11	.4	Diebaart, Ol-Barn, Historiyork, Kiscon
17	21	hily	ad11	A	Diffiely, Officers, Officerseek, 20100
10	27	hungingin	481	.4	Ol-bangjingin, Ol-ban, Kutatenk, Kuta
10	22	DISE_TECTIONS-21429C	481		CH-DEEL TETREE-DISCO, CH-Tear S. DC-Santaeck, DC-con
17	22	1040,7107000-21429C	+81		DEDUK, SETTING-CLOCK, OF THE P. R. CONTROLS, DOI: 10

选择一个目录服务,点击"**添加成员**",系统将从该目录服务读取 用户资料,并以列表形式列出,管理员可从列表中选择成员或组加 入用户组。

点击"添加成员"按钮后,将连接目录服务进入目录浏览界面:

NABH II			
87382	88.		
1.884	403		
£200	delibrations), delibre		
120464	Offices, Ellisticals, Ellise		
HE 1-0			
The second		29 8 8 8 F	
1000	80 85276		
1115			
0	/ Because and	Widowseene, Whee, Elisabet, Elisa	
F	and part	Bradige, Britan, Ernstock, Kros	
F-	ADME	IPoDMI, Orline, Retetersk, Retar	
F	antes .	18-Surge, 1875ers, 27 Sublick, 82 sus	
E:	Sec	Oblast, Oblast, Kristerik, Krim	
c	MOL	Dhile, Offices, Kristianik, Brian	
r.	Some instant	Blangings, Black, Elsowed, Elso	

此时选择你要添加的用户及组,再按"添加选择的项目"按钮,将 你所选择的项目添加至用户组。此浏览界面根据目录服务器中的所 有用户和组的位置关系,以列表形式展开,每个用户及组都有唯一 的目录路径,通过这个路径,在认证时进行定位。

点击应用的策略的"**查看及编辑**"按钮,进入应用策略的配置界面



用产组		
ad_group 应用	的策略 画版	
完全教护		444
访问控制	推出主章符行	+ (************************************
事法外乘管理		66.62
<b>多约卡限制</b>	test2	
甲计加电		6056
101.001	184.	
打印解社	ET RTMRS+	

在此界面中会显示已经应用到此用户组的策略的列表,要将策略加 入此用户组,请点击相应模块的"编辑"按钮,进入策略选择界面

用户组
ad_group 应用的策略
安全防护 金羅來和 三進丹教師
伊德出金蜀鲸行
□ 但允许某场遗理访问购上编辑
— 我在安全体都自然时代评系统进程访问时上却带
□ 禁止事系统进程访问网上保留
「 尤FMSIBH
「 http://met
□ http://h
「III使用acta的改產出版止
□ talnet连入壁止
「 telnet運出等止
厂用户量果时,连入主席位行
「用户兼要时。深出来算改行
三流景控制

在此界面中会列出己配置的所有对应此模块的策略,需要将某条策 略加入此用户组,只需在这条策略前勾选后保存即可。

## 4.10.2. 配置要点(以AD域为例)

#### 添加目录服务

- 1. 点击"目录服务"中的"添加"按钮,进入目录服务添加页面
- 2. 输入"目录名称"为企业域服务器
- 如果 AD 域名称为 testworl.com,则在目录服务路径中输入"目录服务路径"为"dc=testwork, dc=com"
- 4. "目录服务类型"选择"Active Directory Server"
- "访问用户名"为登录 AD 域服务器所在终端的用户名,"访问 密码"为该用户名所对应的密码
- 6. 在"目录服务器列表"栏中输入服务器 IP 地址为 AD 域服务器



的 IP 地址, 然后点击"**添加服务器**"按钮, 将此 IP 添加到列 表中

- 点击"验证",检查是否配置是否正确,是否能跟目录服务器正 常通信
- 8. 点击"保存",保存此目录服务配置

#### 添加用户组

- 9. 点击"用户组"中的"添加"按钮,进入用户组添加页面
- 10. 输入"用户组名称"为财务部
- 11. 点击"用户组成员"的"查看及编辑"选项,进入添加用户组成员界面
- 12. 在"**目录服务**"下拉列表中选择企业域服务器,然后点击"**添** 加成员"
- 13. 进入"目录浏览"页面后,选择 0U 中财务部的用户 testuser1, 点击"添加选择的项目"对所选择的用户加以保存
- 14. 返回上一级目录,点击"应用的策略"的"查看及编辑",进入选择策略界面
- 15. 选择"访问控制"中的"httptest"策略,点击"保存"
- 16. 返回上一级目录后,再次点击"保存"按钮,完成"用户组" 策略的编辑修改

# 4.11. 可信 MAC

\*该章节功能仅适用于高级版和增强身份认证高级版

## 4.11.1. 配置介绍

可信 MAC 组合认证配置界面。在网络准入中如果启用可信 MAC 认证,那么只有列表内的 MAC 地址才能通过认证;在 IP 组中如果启用可信 MAC 认证,那么只有列表内的 MAC 地址才是符合安全基线要求的。



可信MAC管理 添加	]		
<b>《信和</b> 《蒙略列表	÷		
1428	描述	创建者	
Tillese 1		yyhop	

### 点击"添加"按钮,进入可信 MAC 策略配置界面

可信MAC		
可信MAC策略	ş	<u>帮助</u>
策略名称:	可信mac 1	*
策略描述:		A
		<b>v</b>
MAC不存在时:	• 不满足安全状态 〇 满足安全状态	
本策略MAC列表	查看及编辑	
	保存 删除 取消	

配置项:	<u>说明</u>
策略名称	填写策略名称
策略描述	填写对策略的详细描述
MAC 不存在时	选择客户端 MAC 地址不在此列表内时, 客户端是否认为其满足安全基线要求, 如果选择不满足则会在客户端给出提 示,如果选择满足则会认为此客户端是 符合安全基线的。
本策略 MAC 列表	对 MAC 列表进行维护

点击"本策略 MAC 列表"的"查看及编辑"选项,进入添加可信

### MAC 地址界面

<b>自由可信EAC</b> 地址	本加 从振波导入	从文件导入 导出	下载模板 拒國
ACTENT.	主机出口	VLAB Ers Aci	有效期限制
000:29525644	WINTF-CC-IF154	0	青
002215005+54	LINENORE-344585	0	*
0028185 (4050	BABBERTAF	0	香
458taas28200	刘ið-PC	0	香
000+29494427	TESTWORE-XFERV	0	香
000+299014+1	TESTWORE-21429C	0	8
001847-01644	JING-2029029654	0	晋
001-0006-000	778	0	*

点击"**添加**"按钮

1



TEMAC			
添加可信MAC地址			4125
mucie社	1	· 杨庆 : AADGOCDORETT	
ERS:			
maci地址有效有新教	** C #		
auci也让有效期起和的间	2008-3-3-10(14)14	- C3	
NACI推址有效期始来时间	2000-0-0 10174174	- CH	
4002.112法项 VLASTD	0	(0表示不使用此项)	
EDU选项 ACL	无	•	
注:右辺育+号的项目必须输入。			
	保守 潮泊		

配置项:	<u>说明</u>
MAC 地址	填写可信任的主机 MAC 地址。
主机名	填写主机名,便于查询管理。
MAC 地址有效期限制	开启 MAC 地址有效期限制, MAC 地址只 能在指定的时间范围内通过认证,超出 时间范围将被拒绝。
MAC 地址有效期起始时间	MAC 地址有效期起始时间。
MAC 地址有效期结束时间	MAC 地址有效期结束时间。
802.1X 选项 VLANID	为 MAC 地址分配 VLAN,客户端通过认证后,所接的交换机端口将被自动划分 至指定的 VLAN。
EOU 选项 ACL	在 EOU 认证中,以 MAC 地址为目标,向 该客户端所接的交换机端口下发动态 ACL。

点击"**从报表导入**",通过客户端报表中的主机名和 MAC 地址进

行添加



日本市市は	(東 あが的時日	0.0.00000	2 2261	WHEN PURCHASE
-	1.6.1	and the second s	MAR	
111	JIANOR	CB-0753	00-05-10-be-b1-0e	
10	JIAH		00-10-63-60-16-44	
61	明月中中	NO	00-1+-90-50-+0-05	
21	428-21-	0100EA	00-01-29-52-54-94	
8	#19DOM	01058A-T1	00-04-50-40-94-33	
10	BARREN	TAE	00-1+-90-90-s0-T+	
111	ADMINIS	57-636764	00-01-29-58-5e-17	
171	ADMIRTS	T-CP28AS	00-01-29-+b-6e-bb	
101	128-127	568308000	00-01-29-06-91-66	
173	LINDO	NE-230707	00-0+-29-51-61-42	

通过选择的 IP 组和是否绑定的条件进行查询,在查询出的列表中 对需要的绑定项打勾,然后点击"保存选择的项目",对这些 MAC 地址进行保存。

注意:绿色显示的 MAC 地址已经添加到了可信 MAC 列表中。

点击"**从文件导入**",通过固定格式的 EXCEL 文件,导入到数据 库中,对可信 MAC 进行配置。

点击"**下载模板**",将固定格式的文件导出至电脑中,通过修改此 文件对可信 MAC 列表进行维护,再通过"从文件导入"选项,将 维护好的文件导入至数据库中。

## 4.11.2. 配置要点

- 1. 点击"添加"按钮,进入可信 MAC 添加页面
- 2. 输入"策略名称"为认证 MAC 列表
- 3. "MAC 不存在时"选择"不满足安全基线"
- 点击"本策略 MAC 列表"的"查看及编辑"按钮进入 MAC 地址编辑页面
- 点击"从报表导入",选择服务器为"CenterServer",所属 IP
   组为"所有 IP 组",点击"查询"
- 6. 在查询出的列表中选择所需要的 MAC, 点击"保存选择的项目"



7. 返回上一级目录,点击"保存"

# 4.12. 可信 GUID

\*该章节功能仅适用于高级版和增强身份认证高级版

## 4.12.1. 配置介绍

可信 GUID 组合认证配置界面。在网络准入中如果启用可信 GUID

认证,那么只有列表内的GUID才能通过认证;

点击"添加"按钮,进入可信 GUID 策略配置界面

<u>可信GUID</u>	
可信GUID策	略
策略名称	*
策略描述	
创建状态	全局
创建者	administrator
	保存取消

配置项:	<u>说明</u>
策略名称	填写策略名称
策略描述	填写对策略的详细描述

添加完成后的页面如下所示:

可信GUID			
可信GUID策略 可信GUID策略列表	添加		
策略名称	描述	创建者	<u>市叫</u> 設置
gui d	guid	administrator	1

点击"设置"下的" ┙ "按钮"选项,进入添加可信 GUID 地址



新加可信CUID 从报表导入 从文件导入	合忠 英国		
CEL13	TRE	VI.AN	有效规程的
(AC018000-A987-4380-83A1-8200FC9442FF)	liak-0753	0	1
80724004-2820-4907-A008-025601536030	广州连城镇急技	0	書
(7374C5AE-6214-414E-8825-47533D4B1812)	jing text_name	0	膏
07953183-8809-4888-8508-058088378544]	pure-HC	0	<b>T</b>
[07447A86-FE33-41A8-82C3-1530839E97P6]	INSTYLEV-PC	0	-

点击"从报表导入",通过客户端报表中的主机名和 GUID 地址进

#### 行添加

ENTER .	185	TIM	0.07.000.00
ACOUNTS-AND-AND-BEAT-ROOMCDARSHT	1.inle-0753	0	7
[89974034-280]-#997-4003-00580(536030]	广州国杨能皇扶	0	8
[T3P4C5A8-6214-4148-8825-4P5330481012]	jing test aways	0	*
007450273-0079-000-0507-055085308544]	para-90	Ū.	8
[01441A36-FE12-41.60-E012-1531030EV1P6]	DADITLIP-PC	0	
1			
No. 01 - 10 - 10 - 10 - 10 - 10 - 10 - 10	ম		
acriter: 28	1 64		
ET A SULT			
保存选择的项目 保存所有的项目	#.HI		ALL CACE IN
1 000 C	IRS		
C (42066924-353C-4389-4253-5030179124513)	0753-18510600	-00+0e	-29-16-32-wa
- 0940839319-CBSE-4PC9-4548-5865201034801	ADM19-BA2130069	.00-0e	29-66-54-18
CARDERS-0114-4620-0426-430480040188	LEWOP18L-2000	-10+6e	-29-30-38-00
- (#9323.463-82.40-4485-8656-2005.05829982)	AAAAAAA	.00-0e	29-4e-16-ea
- 029670708-4802-4017-8687-3838821052381	LEBUYD-V750H147	.00-0e	29-67-60-13
- 611499120-2040-0150-8882-9014289990121)	TZE-CEOR/FAST64	00-0 e	20-14-46-15
011124014-0120-4140-4008-0054015360301	<b>FRAMALH</b>	in-te	90-96-a0-Ta
P 26002053-4P54-4673-6P57-38030PC38082	(10.9K)Z	00-1e	-25-96-0c-69
CITANTAN-FEIS-4LAS-8213-1530830891761	DATTILIV-HC	00-26	10-66-40-44
			101-10-4 August
[- (1X383630-3480-4851-6720-51A280AC3A89)	ADMENDET-CF2DAS	00-04	41.15.48.00

根据所属 IP 组 和是否绑定的条件进行查询,在查询出的列表中对 需要的 GUID 打勾,然后点击"保存选择的项目",对这些 MAC 地址进行保存。

注意:绿色显示的 GUID 已经添加到了可信 GUID 列表中。

点击"**从文件导入**",通过固定格式的 EXCEL 文件,导入到数据 库中,对可信 GUID 进行配置。

点击"下载模板",将固定的 GUID 导入格式的文件导出至电脑中,通过修改此文件对可信 GUID 列表进行维护,再通过"从文件导入"



选项,将维护好的文件导入至数据库中。

注意: GUID 认证仅支持标准 802.1x 与漫游 802.1x

## 4.12.2. 配置要点

- 1. 点击"添加"按钮,进入可信 GUID 添加页面
- 2. 输入"策略名称"为认证 MAC 列表
- 点击"本策略 GUID 列表"的"查看及编辑"按钮进入 GUID
   地址编辑页面
- 点击"从报表导入",选择服务器为"CenterServer",所属 IP
   组为"所有 IP 组",点击"查询"
- 在查询出的列表中选择所需要的 GUID,点击"保存选择的项目"
- 6. 返回上一级目录,点击"保存"

# 4.13. 用户、IP、MAC 组合

## 4.13.1. 配置介绍

通过客户端的 USER-IP-MAC、MAC-IP 的组合绑定,对客户端进行唯一性检查,只有符合绑定要求的客户端才符合安全基线的要求。 USER-IP-MAC 可细分为 User-IP, User-MAC, User-IP-MAC, User4 种组合。

点击"添加组合策略"按钮,进入组合管理策略配置界面



用户、IP、MAC組合		
组合策略		<u>帮助</u>
组合策略名称		*
策略描述		
组合不存在时	· ○ 不满足安全基线 · ● 满足安全基线	_
请选择一种组合类型	USER-IP-MAC组合	¥
注:右边有*号的项目	必须输入。 保存 取消	

配置项:	<u>说明</u>
组合策略名称	填写简单明了的组合策略名称。
策略描述	详细策略描述
	当选择 User-IP-MAC 组合时,登录用户在
御人不安を吐	组合中不存在;或选择 MAC-IP 组合, MAC
	在组合中不存在,这两种情况称为组合不存
和日小升红的	在。在组合不存在的情况下,可以采取"不
	满足安全基线"和"满足安全基线"两种认
	证操作。
	选择组合类型,包括 User-IP-Mac 以及
<u> 选择</u> 一种组入米利	MAC-IP 组合两种。User-IP-MAC 以 User
心并一件组百天望	为检测的对象,MAC-IP组合以MAC为检
	测的对象。

组合管理	漆加	<b>电合策略</b>		
细合氯明名称	194	1162 <b>5</b>	國家者	1241a
21212		USER-17-MACI且会	luerhuojun	1
a		10700-15-01-08-0	Acres See	

点击"保存"对所配置策略进行保存,保存后的页面如下图所示:

## USER-IP-MAC 组合



点击已保存的策略名称,进入策略修改界面

组合策略	
组合策略名称 21212	*
策略描述	
组合不存在时 ◎ 不 请选择一种组合类型 USER- 注:右边有*号的项目必须输 保存	第日安全状态 ◎ 第日安全状态 IP-MAC组合 ▼ 入。 開除 取消
点击 " <b>设置</b> " 下的 " 🥒	"按钮"选项,进入绑定策略设置界面
设置组合策略 "21212" <sup>用户名</sup> IPIN	· 查询 · 业图 · 美国
已设置的用户 用户名 日前正约案件 1	的症状态 创流的 YIAN 网络
- 选加用户 从报表添加 A	文件导入 导出 下航导入模板
配置项:	<u>说明</u>
添加用户	通过配置页面手工添加组合设置。
儿 把 丰 沃 <del>加</del>	系统自动读取客户端报表信息,管理员可从
MJK-花松M	中选择添加组合设置。
以文件导入	使用组合导入工具,将 Excel 文件中的组合
水人开サ八	信息导入系统数据库。
导出	将组合信息导出至 Excel 文件。
下载导入模板	下载用于文件导入的 Excel 模板。

**注意**:通过"用户名"或者"IP 地址"的查询,可对所绑定的信息进行快速查询,且在进行绑定设置时,如果出现重复绑定的 IP 地址,程序会自动检测,并给出提示。

点击"**添加用户**",进入用户添加界面

E



设置组合策略"	100 ~	
电户基本信息		With
<b>用户</b> 名		
<b>建</b> 养后;		
s/1:		
日東線条路径		
	₩ 部略日意服务路径	
·····································	α	仅在启用602 La网络维入时生效
BSAT.		<u></u>

配置项:	<u>说明</u>
用户名	填写 LDAP 目录服务中的用户名,可为中文或 英文。
登录名	填写LDAP目录服务中的登录名,一般为英文。 AD域的登录名在整个域里面都是唯一的,而 IPlanet和 OpenLDAP 的登录名在域里可以有 重名,重名的登录名以目录里的 OU 区分。
部门	填写 LDAP 目录服务中的部门 OU,可不填
目录服务路径	填写此用户的完整 DN 信息,如 test 用户的完整 DN 是: 整 DN 是: CN=test,CN=Users,DC=Sample,DC=com,那 么此处填写的路径 CN=test,CN=Users,DC=Sample,DC=com。注 意目录服务认证时对大小写敏感。
忽略目录服务路径	如果目录服务中的登录名是唯一的,不需要 通过目录服务路径来区分,您可以选择忽略 目录服务路径。(AD 的登录名是唯一的,对 其他的目录服务您可以通过规划保证登录名 是唯一的)



	为此用户绑定动态 VLANID,用户认证后可
动态 VLAN ID	自动将交换机端口划分至绑定的 VLAN。此
	功能仅在启用 802.1x 网络准入时生效。
	为此用户绑定动态 ACL, 用户通过 EOU 认证后
动态 ACL	可自动向交换机下发动态 ACL。此功能仅在启
	用 EoU 网络准入时生效。

点击"保存"后,对此用户的设置进行保存

**注意**:如果选择"忽略目录服务路径",请在输入"用户名和"和 "登录名"时与目录服务中的保持完全一致,否则可能出现认证不 通过的情况。

点击设置好的用户信息名称,进入后会出现"组合关系"的设置选项

C BE ON FL DICHE		
制户基本信息		MAL
肥产者	administrator	—,
単発名 〒	administrator	
8/]:		
<b>予职务</b> 路径		
	12 高級目子部各執行	
BEVLAN ID	0	仅在启用002 La門時億入时生效
bäact.		3
		技在启用时间招推入财业效
88关系	查查汉病语	

点击"组合关系"的"查看及编辑"选项,进入 IP-MAC 绑定策略

#### 配置界面

受置组合策略	"100 "			
	·"的IP及IMC组合关系	k		MBh.
and the second se				
手工地加工	F 及RAC 组合关系	形刻		
于工地加加 MACINA	F 没用AC组合关系 LIVIAN	取 に 将 ズ	17.21	#改组合天本

点击"手工增加 IP 及 MAC 组合关系"按钮



<u>用户、IP、MAC</u>	<u>組合</u>		
设置组合策略"100"			
"administrat	tor"的IP及∎AC組合关系		
用户名	administrator		
目录服务路径			
MAC地址		🥒 🗹 不暇	格式:AABBCCDDEEFF
IP地址限制	●否○是		
IP地址类型	静态IP地址		
IP地址			
子网掩码	255.255.255.0		
默认网关			
有效期限制	●否○是		
有效期起始时间	2009-9-14 17:00:58		
有效期结束时间	2009-9-14 17:00:58		
	保存删除取消		

输入所需绑定的 IP 及 MAC 地址等信息

配置项:	<u>说明</u>
MAC 地址	决定是否将 MAC 地址为组合认证条件。准入认 证时客户端的 MAC 地址必须与组合内的 MAC 地 址一致才可通过认证。
IP 地址限制	决定是否将 IP 地址为组合认证条件。
IP 地址类型	设置组合认证条件中 IP 地址的类型,包括 DHCP 和静态 IP 两种。
IP 地址	准入认证时客户端的 IP 地址必须与组合内的 IP 地址一致才可通过认证。
子网掩码	子网掩码不作为组合认证条件,仅在系统根据 登录用户的User-IP组合自动更正客户端 IP地 址时,用于修改子网掩码。
默认网关	默认网关不作为组合认证条件,仅在系统根据 登录用户的User-IP组合自动更正客户端 IP地 址时,用于修改默认网关地址。



	设定组合规则的有效期,如果超过有效期,对
有效期限制	网络准入,则认证不通过;对于非网络准入,
	则此条规则无效。
有效期起始时间	有效期起始时间。
有效期结束时间	有效期结束时间。

点击"保存",完成 USER-IP-MAC 绑定配置

点击"**从报表添加**"按钮,可以从已知的客户端报表信息中添加绑 定策略

() () () () () () () () () () () () () (	単体課題編奏員: 単体課題的に相: 已経現家: 1.165.単	CenterServer  FWIPH  EH	3		6.MI		
- 4	出海燕英/黎南 出历有页/取两	adl 1	• 0	<b>改造者的項目</b>		8829	
1	IKS.	15		ITIME	1118.16.15	strin termini	MX
F	L1007188- 344523		002215006-54	192, 168, Q. 181	PORE	205 225 225 0	190, 166, 0, 1
r	LIUTAR		00242+se:1634	192, 198, 0, 195	學習諸並	285.255.255.0	192,168,0,1
F	TESTECRE- 214290		000.098550.07	192.000.0.194	958¥	255,255,255,0	192 160 D I
r	1180- 2029029854		0018£3+01944	192, 188, 0, 198	發出後於	298-298-299-0	192, 168, 0, 1
	DATERNIAN	(The Protector Statistics	000510574050	192 100.0.203	MARK!	255.255.255.0	192 168 0 1

选择需要绑定的主机,并选择对应的目录服务,点击"**保存选择的** 项目"进行绑定操作。

**注意**:只有向中心策略服务器上报过客户端信息的终端才会出现在 列表中,如果"用户"栏是空的,说明这台终端没有登录过目录服 务,因此需要在保存后再对其进行手工修改。

### MAC-IP 组合

配置 MAC-IP 组合与 USER-IP-MAC 组合类似,点击已保存的策略名称,进入策略修改界面



<u>用户、IP、MAC组合</u>		
组合策略		
组合策略名称	mac-ip *	
策略描述		~
		~
组合不存在时	◉ 不满足安全状态 💿 满足安全状态	
请选择一种组合类型	MAC-IP组合 🔹	
IP绑定生效范围	◎ 所有网络环境生效	
	◎ 仅在所属管理网段生效	
	◎ 仅在本IP组生效	
注: 右边有*号的项目	必须输入。	
	保存 删除 取消	

点击保存后,出现如下页面:

组合管理	-5.htt	自合筆電		-
uansee	<b>N</b> ie	862 <b>2</b>	创建办	教育地会
21212		11223-17-86Ci8A	luerkeejan	1
212		WSER-12-MAC组合	luorkosjan	2
fdafadf		WAC-IP協会	jing	1
		WAC-IP细合	jing	1

点击"**设置**"下的" ✔ "按钮"选项,进入 MAC-IP 绑定设置界

面

VH al i X	d macy ip			
el	BAC		第二章 第二章 第二章	
」设置的MAC-12地	並組合列表	S		¢
214D	BACIE IN	11/10.10	LENN AND	
002215005-854	002215005+54	192.168.0.181	静态口地地	×
00242car1634	00242cac163d	192.168.0.185	静态口的数	×
000-2989550-07	000-298550.4T	192 168 0 194	静志环地址	×

配置项:	<u>说明</u>
添加	通过配置页面手工添加组合设置。
从报表增加	系统自动读取客户端报表信息,管理员可从中 选择添加组合设置。



从文件增加	使用组合导入工具,将 Excel 文件中的组合信 息导入系统数据库。	
导出	将组合信息导出至 Excel 文件。	
下载导入模板	下载从文件增加功能所使用的导入模板。	

点击"添加"按钮,手工添加 MAC-IP 绑定策略

88	ľ	•这个古银子作为以近的单位,仅作为你学习这个1960的形式
HACHRAE	1	· MIC : MARCINETY
171636(5)30	· Mathematic Canatanata	
THEF		
子門地站	1	•
利式	1	
#10	-	2
		-
T TORER OF	ANC.4	
# 11 MET F10710	0009-9-14 18:00:10	19
W TH REA WORTH	2009-9-14 18100110	
E: 如识有+等4501日	eran.	
	16.7F	

配置项:	<u>说明</u>
名称	您能记住的名字。一般以主机名或使用者的名字作为名称,名称不作为认证条件。
MAC 地址	系统以这个 MAC 地址为基准, 对其对应的 IP 地 址进行验证。
IP 地址类型	设置组合认证条件中 IP 地址的类型,包括 DHCP 和静态 IP 两种。
IP 地址	准入认证时客户端的 IP 地址必须与组合内的 IP 地址一致才可通过认证。
子网掩码	地址掩码不作为组合认证条件,仅在系统根据 MAC-IP 组合自动更正客户端 IP 地址时,用于修 改地址掩码。
网关	默认网关不作为组合认证条件,仅在系统根据 MAC-IP组合自动更正客户端IP地址时,用于修 改默认网关地址。

描述	关于组合规则的进一步描述。	
有效期限制	设定组合规则的有效期,如果超过有效期,对 网络准入,则认证不通过;对于非网络准入, 则此条规则无效。	
有效期起始时间	有效期起始时间。	
有效期结束时间	有效期结束时间。	

点击"保存",完成 MAC-IP 绑定

也可点击"从报表添加",从客户端报表中选择需绑定的终端进行 MAC-IP 绑定

	anne	000-29655047	192.16	0.0.194 🖬	atorina ta	×	
1	im Affin	8.M M.S	(P-W)M 52:	8 F&9A	12.65		
日本の	n munimentati sa ana a Ta numuna seconda a Ta Elaberati a Ta	end er Seitrer F Wilt-W E MS	1	- -			
	·法当和五/除油	保存法非约束	10 E51	]		NACE OF	制化的建筑和
1	148		1216.001	HLP BUI	山井市	COMPANY OF PA	ALC: N
-	12819064-344633	002219005-54	192, 160, 0, 101		<b>新空体</b> 线	295 255 255 0	192,168,0.1
e	ALCOHOM .	00042+4+0834	102.168.0.199		兼设地址	255 255 255 0	195,168,0,1
e	TETRIKE-SHOPE	000-099996-07	192 188 0 194		8-54th	1996 1996 1996 0	102 100 0.1
-	JUN-2009054	001863-01944	192, 188, 0, 199		静密地址	295 295 295 0	192 164.0.1
				a a second concernant	marine		
r	BARRENTAN	002619664050	192, 168, 0, 203	amentstraticBall1	聯合增加	294-288.256.0	192.198.0.1

## 4.13.2. 配置要点

- 点击"添加组合策略",输入"组合策略名称"为U-I-M组合策
   略
- "组合不存在时"选择"不满足安全基线",并选择"USER-IP-MAC 组合",并点击"保存"
- 点击策略名称 "U-I-M 组合策略",进入后点击"设置组合"中的"查看及编辑"
- 4. 点击"从报表添加"按钮,选择好所属服务器及 IP 组,点击"查 询"
- 5. 在用户列表中找到用户"Darren@ad11",并勾选此用户,再选



择目录服务为 "adl1", 点击 "保存选择的项目" 进行保存

- 点击用户名 "Darren",进入 "用户基本信息配置" 界面,并点击 "组合关系"的 "查看及编辑",进入组合关系设置界面
- 此时这个用户已绑定一个 IP 地址,可点击"手工增加 IP 及 MAC 组合关系",绑定此用户使用的其他 MAC 和 IP
- 取消"MAC 地址"的"不限"的勾选,并输入 MAC 地址为
   "0026186f4050"
- 9. "IP 地址限制"选择"是","IP 地址类型"选择"静态 IP 地址",并输入"IP 地址" 192.168.0.18,"子网掩码"为 255.255.255.0,默认网关为192.168.0.1,"有效期限制"选择"否", 并点击"保存"
- 10. 此时使用"Darren"用户登录,MAC地址为"0026186f4050"
  的客户端的IP地址会被绑定为192.168.0.18,而如果用"Darren"
  用户登录的客户端的MAC地址不对,客户端会提示您"不符
  合安全基线要求"。

# 4.14. 网络设备配置

\*该章节功能仅适用于高级版和增强身份认证高级版

网络设备配置是配置准入控制的交换机或者路由器设备。

在网络准入配置中将已配置好的网络设备关联到 radius 服务器中。参考《网络准入-〉Radius Server》的配置

#### 网络设备配置页面

点击"网络设备配置" 中的 "添加"可添加新的交换机或者是路由

也可点击"网络设备配置"中的"导入" 导入交换机或者是路由器的配置 信息。

器:



195 04 199 10		44E	5800	 2008	Destrain 1	-
	Antalas	MARK RALLET	¥ #19804			
	C un contrato C un contrato C un contrato					
USALINE	THE OWNER AND A DESCRIPTION OF A DESCRIP					
benuete			(+)			
510						
Recent	H LAP 12 KL	ar.				
N早田18						
Revert	MR					
网络会会品牌	34.95					
网络设备业地址		1.0				
网络杂香油粉						
100.0010.0010						

配置项:	<u>说明</u>		
网络设备名称	对该网络设备命名		
网络设备 IP 地址	该网络设备的 IP 地址,用于提供对该网络设备 认证支持		
网络设备品牌	所添加网络设备的品牌;填写此项方便端口绑 定及端口识别,如果需配置端口绑定,则一定 需要填写此项。如果选择"其它",则暂时不 支持端口绑定。		
网络设备型号	所添加网络设备的型号;填写此项方便端口绑 定及端口识别,如果需配置端口绑定,则一定 需要填写此项。如果选择"其它",则暂时不 支持端口绑定。		
共享密钥	有线以太网交换机网络准入认证标准为 EAP-MD5(Challenge)认证,加密认证双方需 要有相同的密钥。		
网络设备类型	网络设备类型; LAN 即有线以太网网络设备, 如: CISCO 3560; WLAN 即无线以太网网络设 备,如 TP-link 无线 AP		



GGID	SSID 用来区分不同的无线网络,只需在无线网
SSID	络中配置此 ID 号。
	天珣网络准入同时支持基于用户信息、MAC 地
	址的动态 VLAN 切换。但不同的厂商 VLAN 格
-1-4- 573 -+-4+	式不同,例如 Cisco 交换机的 VLAN 号是字符
动念 Vlan 文持	串形式,而H3C(原华为)交换机的VLAN号
	是数字形式。请根据具体交换机的厂商选择。
	目前版本不支持锐捷交换机的动态 VLAN
	支持对交换机上的端口进行绑定特定的 MAC、
	IP、GUID 以及登录的用户名。可以手动添加绑
	定,也可从接入交换机(或者路由器)正在准入的
	客户端信息中导入。如:对交换机 0/0/3 端口唯
	一绑定终端 MAC:60EB69F14F53,
	终端 GUID:
	{E0C5B2C8-A61A-4F36-84C3-2DCB9B1EA882
	},登录名称为:happy,则只有当接入该端口的客
	户端满足这三个条件且安全状态满足时,网络
IAN港口独宁	才能连通
LAIN 圳口外化	共有三个选项:
	"不启动端口绑定,端口使用不受限制":则不
	启用端口绑定功能,下面的绑定条目编辑框处
	于不可编辑状态
	"端口仅限绑定的终端使用,未设置绑定的端
	<b>口不受限制"</b> : 绑定的端口只允许被绑定的客户
	端通过,其他客户端拦截;未设置绑定的端口
	正常使用,不受限制
	"端口仅限绑定的终端使用,未设置绑定的端
	口禁止使用": 绑定的端口只允许被绑定的客户



端通过,其他客户端拦截;未设置绑定的端口
如果开启了802.1x认证,则对所有的客户端都
拦截

# 4.15. 分组信息

## 4.15.1. 配置介绍

# 4.16. 全局参数

## 4.16.1. 配置介绍

全局参数分为两部分:"客户端全局参数"和"服务器全局参数"。 通过这个配置来确定客户端及服务器的一些开关性质的内容和最 基本的参数,此处的参数决定策略系统的运行方式和后台交互的频 度,以及全局范围内的默认设置。

### 客户端全局参数

客户端注册参数: 修订			改	
是否启用客户端注册			否	
对以下日期前注册的客户端,要求重新注册			1970-01-01	
客户端注册重复提示周期			不重复提示	
客户端注册项目			Email: 地址: 电话:	
配置项:	说明			
	00/1	1		
是否启用客户端注册		设置是	否要启用客户端注册	
对以下日期前注册的客户端,要		对超过一定注册时间的客户端		
求重新注册		设置时	间要求其重新注册	
		定时在	客户端提示进行注册,	若
客户端注册重复提示周期		不注册	将会在这个周期时间后	1
		再一次	z 提示注册	



	设置客户端注册填写的项目,包
	括其顺序、是否必填项目和是否
今日淮沿司站口	作为查询条件(在信息中心-资
各广场注劢坝日	产信息查询作为条件查询),默
	认项目为 email、地址、电话(这
	3项不能修改或删除)

客户端访问控制:	<u>修改</u>
默认访问控制操作类型	放行
毎客户端总帯宽限制(OKB/s表示不限制)	不限制
默认的访问控制日志方式	总是记入日志

配置项:	<u>说明</u>		
	共有3种默认操作		
	放行:对没有规则匹配的数据包放		
	行。		
	放行并让用户确定以后的操作:先放		
	行没有规则匹配的数据包,然后在客		
默认访问控制操作类型	户端弹出一个对话框,让用户确定以		
	后将如果处理相同的网络访问。		
	不放行并让用户确定以后的操作:先		
	拦截没有规则匹配的数据包,然后在		
	客户端弹出一个对话框,让用户确定		
	以后将如果处理相同的网络访问。		
	客户端防火墙会对每个连入和连出		
	的数据包进行流量统计,但会排除那		
每家白光台带金阳制	些注明不计入总流量的网络访问。在		
<b>举合广</b>	一般的设置中,每客户端总带宽限制		
	用来对非业务流量进行一个"封顶"。		
	可以按照带宽的绝对值(KB/S)或		



	网卡带宽的相当值(%)来进行设置。
	每一条访问控制规则都可以覆盖此
默认的访问控制日志方式	处设置的日志方式,也可以使用此处
	设置的默认日志方式。

**注意**:在客户端防火墙对客户端的网络数据包进行策略匹配时,如果不能匹配任何访问控制策略,则使用此处设置的默认访问控制操作类型对数据包进行处理。这里的默认访问控制类型是全局的,IP 组或安全防护用户策略组中的默认操作类型可以覆盖这里的设置。

客户端日志参数:	<u>修改</u>
是否将网络行为日志发送给服务器	是
配置项:	<u>说明</u>
是否将网络行为日志发 送给服务器	设置客户端的网络行为日志即防火墙日 志是否发送给服务器,选择是的话,将 会在信息中心查询到策略事件的详细信 息



客户端运行参数:	<u>修改</u>
客户端日志缓存文件大小	32768 KB
防火墙日志文件大小限制	100 KB
重新从Server上下载策略的时间间隔	24小时
主动探测非受控终端的在线状态 (建议终端数大于200的VLAN关闭主动探测)	否
客户端DNS设定(不生效)	无
客户端WINS设定(自动修改IP地址时使用)	无
服务中心WEB站点URL	
检测Windows弱密码	否
启用对本系统客户端注册表项的保护(64位系统无效)	否
客户端启用802.1x认证	是
启用Windows自带的802.1x认证	否
是否启用客户端与服务器之间的时钟同步	否
时钟源	无
NTP Server地址	无
禁止用户修改Windows时间	否

配置项:	<u>说明</u>
客户端日志缓存文件大 小	客户端 audit.dat 记录了客户端的审计及 告警日志信息,文件默认为 32768 KB, 可以通过该选项修改该文件大小。
防火墙日志文件大小限 制	设置客户端的防火墙日志大小;防火墙 日志默认为100KB,可更改。如:防火墙 日志设为100KB,则当防火墙日志大于 100KB时,则自动备份,再新生成一个 客户端防火前日志文件
重新从 Server 上下载策 略的时间间隔	如果客户端一直处于运行状态,客户端 将每隔一个固定周期向服务器重新下载 策略规则。默认值为24小时。客户端每 次启动后都会自动下载策略规则。
主动探测非受控终端的 在线状态	如果选择了主动探测非受控终端的在线 状态的话,终端会定时发送数据包确认

	非受控终端是否在线,默认为不启用。
	但如果用户子网较大或者交换设备性能
	较差的情况下,可能导致交换机负载过
	高的问题,此时可以选择取消主动探测
	非受控终端的在线状态。
	如果设置了 MAC-IP 绑定和 User-IP 绑定
	策略,当客户端的 IP 地址与绑定的 IP 地
客户端 DNS 设定	址不符时,系统会自动将客户端的 IP 地
	址改回到绑定的 IP 地址。并将 DNS 设置
	为此处输入的 IP 地址。
	如果设置了 MAC-IP 绑定和 User-IP 绑定
	策略,当客户端的 IP 地址与绑定的 IP 地
客户端 WINS 设定	址不符时,系统会自动将客户端的 IP 地
	址改回到绑定的 IP 地址。并将 WINS 设
	置为此处输入的 IP 地址。
	客户端用户界面有一个"服务中心"按
服务中心 WEB 站点	钮,当用户点击这个按钮时,会打开一
URL	个新浏览器,并自动访问此处设置的
	URL.
	客户端会使用弱密码不断尝试登录
	Windows, 如果可以登录就说明该用户属
检测 windows 弱密码	于弱密码并上报弱密码。如果 windows
	策略中有设置帐号锁定策略,请关闭该
	功能,即选择为否
启用对本系统客户端注	对本系统在客户端上所注册的注册表项
册表项的保护	进行保护,防止非法修改和攻击
客户端启用 802.1x 认证	让客户端上的 802.1x 选项默认开启或关


	闭,如果使用网络准入请选择开启
启用 windows 自带的 802.1x 认证	选择是否启用 windows 自带的 802.1x 认证,如果启用了,那么天珣的 802.1x 认证将会受到影响
是否启用时间策略	选择是否启用时间策略
是否启用客户端与服务 器之间的始终同步	选择让客户端是否同步服务器时间
时钟源	选择同步时间的时钟源,可选择直接与 中心服务器同步或自定义时钟源
NTPserver 地址	若选择自定义时钟源的话,在此处输入 时钟源的服务器地址
禁止用户修改 windows 时间	选择是否禁止用户修改 windows 时间

## 服务器全局参数

服务器全局策略:         修改           服务器汇总报表时间         0时0分           报表中的用户名称         未知           当事受控终端的不活动的天数超过以下值时,自动删除该终端信息         2天           当數据库所在確盘空间少于以下值时,显示字体变为黄色         1024加B           WEB控制台登录参数:            WEB控制台登录参数:            WEB控制台登录参数:            WEB控制台登录参数:            WEB控制台登录参数:            WEB控制台台號         20分钟           允许登录 WEB 控制台的 IP 登录列表         0,0,0,0 - 255,255,2           55,255         255,255,2           55,255         255,255,2           公式            企业LOGO (JPEG或GIF)标准像素860*57            注ULOGO (JPEG或GIF) 微索小于500*40            次览         上传文件           塗束页LOGO (JPEG或GIF) 标准像素350*250	服务器全局参数	<u>春夏助</u>
服务器汇急报表时间 0时0分 报表中的用户名称 未知 当非受控终端的不活动的天数超过以下值时,自动删除该终端信息 2天 当数据库所在硬盘空间少于以下值时,显示字体变为黄色 1024MD          WEB控制台螢录參数:       (2000)         WEB控制台螢录參数:       (2000)         登录失败限制次数 3次       3次         超时退出(注情)的等待空闲时间 20分钟       (0,0,0,0)         允许登录 WEB 控制台的 IP 螢录列表 0,0,0,0)       - 255,255,2         企业LLOGO:       (200)         化比CGO(JPEG或GIF)标准像素860*57       (200)         企业LLOGO(JPEG或GIF)标准像素860*57       (200)         2000(JPEG或GIF)标准像素350*250       (200)	服务器全局策略:	<u>修改</u>
报表中的用户名称     未知       当非受控终端的不活动的天数超过以下值时,自动删除该终端信息     2天       当数据库所在硬盘空间少于以下值时,显示字体变为黄色     1024MD       WEB控制台登录参数:	服务器汇总报表时间	0时0分
当非要控终端的不活动的天数超过以下值时,自动删除该终端信息 2天 当数据库所在硬盘空间少于以下值时,显示字体变为黄色 1024MB WEB控制台登录参数:	报表中的用户名称	未知
当数据库所在硬盘空间少于以下值时,显示字体变为黄色	当非受控终端的不活动的天数超过以下值时,自动删除该终端信息	2天
WEB 控制台登录参数:         修改           登录失败限制次数         3次           超时退出(注前)的等待空闲时间         20分钟           允许登录 WEB 控制台的 IP 登录列表         0.0.0.0 - 255.255.2           企业LOGO:	当数据库所在硬盘空间少于以下值时,显示字体变为黄色	1024MB
WEB 控制台登录参数:         修改           登录失败限制次数         3次           超时退出(注销)的等待空闲时间         20分钟           允许登录 WEB 控制台的 IP 登录列表         0,0,0,0 - 255,255,2           企业LOGO:		
登录失败限制次数 3次     超时退出(注销)的等待空闲时间 20分钟     20分钟     允许登录 WEB 控制台的 IP 登录列表 0,0,0,0 - 255,255,2     55,255     c	WEB控制台登录参数:	修改
超时退出(注詞)的等待空闲时间 20分钟 允许登录 WEB 控制台的 IP 登录列表 0.0.0.0 - 255.255.2 <u>6年北LOGO:</u> //eb控制台Banner企业LOGO(JPEG或GIF)标准像素860*57 ② 览 上传文件 ② 近 上传文件 登录页LOGO(JPEG或GIF)标准像素350*250	登录失败限制次数	3次
允许登录 WEB 控制台的 IP 登录列表	超时退出(注销)的等待空闲时间	20分钟
企业LOGO: Meb控制台Banner企业LOGO (JPEG或GIF)标准像素860*57 ② 览 上传文件 ② 拉LOGO (JPEG或GIF)像素小于500*40 ② 波览 上传文件 登录页LOGO (JPEG或GIF)标准像素350*250	允许登录 WEB 控制台的 IP 登录列表	0.0.0.0 — 255.255.2 55.255
/eb控制台Banner企业LOGO (JPEG或GIF)标准像素860*57 [浏览]上传文件 企业LOGO (JPEG或GIF)像素小于500*40 [浏览]上传文件 登录页LOGO (JPEG或GIF)标准像素350*250	企址L060:	
[浏览]上传文件 ②业LOGO (JPEG或GIF) 像素小于500*40 [浏览]上传文件 登录页LOGO (JPEG或GIF) 标准像素350*250	#eb控制台Banner企业LOGO (JPEG或GIF) 标准像素860*57	
<u>论业LOGO (JPEG或GIF)</u> 像素小于500*40 [浏览]上传文件 登录页LOGO (JPEG或GIF)标准像素350*250		浏览 上传文件
[浏览]上传文件 登录页LOGO (JPEG或GIF)标准像素350*250	企业LOGO(JPEG或GIF)像素小于500*40	
差录页LOGO (JPEG或GIF)标准像素350*250		浏览 上传文件
	登录页LOGO(JPEG或GIF)标准像素350*250	



配置项:	<u>说明</u>
服务器同步报表时间	<ul> <li>设定本地服务器与中心策略服务器之间</li> <li>同步客户端信息和部分报表的时间,默</li> <li>认为凌晨0点</li> </ul>
报表中的用户名称	报表导出成文件时添加这个用户名称, 生成企业独特的报表
当非受控终端的不清 的天数超过以下值时 自动删除该终端信息	后动 计, 默认 3 天 1,
当数据库所在硬盘空 少于以下值时,显示 体变为黄色	至间 示字 默认 2048M
登录锁屏的失败限制 数	可手动设置用户输入错误密码时的尝试 次数。如:设置为 3,则用户有三次机会 尝试输入正确的密码,如果三次都输错, 则禁止再次尝试,锁定登录框
登录锁屏的等待空闲 间	3时 设置 锁定登录框后,用户可再次尝试登录的时间间隔;如:设置为1分钟,则锁屏一分钟后,用户可再次尝试登录
允许登录 Web 控制 IP 登录列表	合的         配置可以访问天珣Web 控制台的IP地址           段,默认对 <u>http://localhost:8833</u> 和           http://127.0.0.1;8833         放行
Web 控制台 Banner 业LOGO(JPEG或( 标准像素 860*57	<b>金</b> Lt传后,在Web 控制台的顶端会出现该 Logo
企业 LOGO	企业 LOGO,上传后,在导出报表时会 将此 LOGO 打上水印
登录页 LOGO	在管理台登录界面显示的 LOG

# 5. 安全基线

# 5.1. 关于安全基线

■ 安全基线是每一台受控终端必须满足的最基本的安全规范。

只有满足安全基线的终端才能正常接入网络,才会被认为是



网络内的合格终端,否则,客户端将会给出提示要求修复。 订制安全基线是通过以下几个策略来实现的:补丁策略,进 程策略,软件安装策略,windows 服务管理,防病毒软件策 略,windows 组策略,屏幕保护策略,共享资源管理,用户 环境策略。

- "补丁强制策略":强制要求客户端必须打指定补丁,确保 客户端的操作系统的漏洞及时修复。比如打一个比较大的 ServicePack或单个的补丁。
- "进程管理策略":对客户端运行的软件和进程进行限制。
   包括红名单,黑名单和白名单。红名单是必须运行的进程列表,黑名单是不能运行的进程列表,白名单是允许运行的进程列表。
- "软件安装策略":软件安装管理可以制定软件安装的红、
   黑、白名单,确定用户客户端必须安装的软件,禁止非法安装未经许可的应用软件,规定只能安装的软件清单。红名单是必须安装的软件,黑名单是不能安装的软件,白名单是允许安装的软件列表。
- "Windows 服务管理" window 服务管理可以禁用或启用客 户端运行的服务。禁止不需要的服务,强制启动需要的服务。
- "防病毒软件策略":通过检查客户端安装的杀毒软件的病毒码,对其所安装的防病毒软件的病毒库更新进行监控。 目前支持的防病毒软件品牌包括 Symantec,趋势,瑞星, McAfee,微软等。
- "Windows 账户策略":账户策略可以修改 windows 管理员 账号、强制禁用 guest 帐号、启用和加强密码复杂度,回收 管理员权限等等来保护系统账户安全。
- "Windows 本地策略":通过修改注册表和组策略的方式, 强制使不安全的客户端满足加固策略要求。例:开启 IP 协议策略可防止 SYN 攻击。

```
■ "注册表策略": 通过检测和保护注册表的方式,保护系
65
```



统的注册表不被擅改。

- "共享资源策略":可以检测并上报用户电脑上有哪些共享资源(目录、打印机、IPC),并可设定是否允许开设共享资源(目录、打印机、IPC),如果不允许,可强制取消已经设置了的共享资源。
- "Windows 事件日志管理":设置 windows 应用程序、安全 和系统的事件日志大小,可查看较长一段时间的日志。
- "用户环境策略":配置安全可靠的用户环境,是否加入域,
   禁止修改网卡、设置屏幕保护等均可提高计算机使用安全系数。

# 5.2. 补丁强制策略

## 5.2.1. 配置介绍

配置补丁强制策略的目的是检查客户端上所打补丁的情况,使每 台客户端上安装的系统补丁都相同,如果有某些补丁未安装的话 将会给予适当的提示要求其安装补丁。

#### ServicePack

Service Pack 是操作系统一个比较大的更新,同时也包含了上 一个 Service Pack 到这一个 Service Pack 之间的所有的 Hot Fix。通过设置强制补丁,能确保终端操作系统的重要补丁都正 常安装。因为 Service Pack 文件很大,而且一般也不需要紧急 安装,所以系统不自动下载 Service Pack,需要您手工配置。 点击"添加"进入 ServicePack 设置界面



Service Pack	Hotfix
SP补丁	
策略名称	*
策略描述	
选择操作系统	₩indows 2000(32位)
ServicePack主编号	**没有ServicePack**
ServicePack副编号	**没有副编号**    ▼
简体中文下载网址	
繁体中文下载网址	
英文版下载网址	
生效时间	◉ 所有时间 ○ 工作时间 ○ 非工作时间 ○ 以下时间段
	开始时间 结束时间 编辑 删除
	2012-03-10 9:00 2012-03-10 13:30 添加
在线模式	☑ 在线时生效 ☑ 离线时生效
策略应用对象	(还没有应用到任何对象) 查 <u>看及编辑</u>
创建类型	全局
创建者	jing
注: 右边有*号的项目必	须輸入。 保存 取消

配置项:	说明
Servicepack 名称	填入补丁的名称,如"Windows XP2"。
选择操作系统	根据不同的补丁,选择相应的操作系统。如选择"WINDOWS XP"。
ServicePack 主编号	根据不同的补丁,选择主编号,如 "ServicePack2"。
ServicePack 副编号	选择相应的副编号,若没有,则不用选 择。
简体中文下载网址	输入该补丁的简体中文版的下载地址。 输入相对地址"XP/ Windows-XP-serviceXP.exe",系统将 自动在相对地址前补充http://服务



	器地址:8833/download/。
繁体中文下载网址	配置同"简体中文下载网址"。
英文版下载网址	配置同"简体中文下载网址"。
在线模式	选择在线和离线时此策略是否生效
生效时间	可以根据管理员的需求,灵活配置策略 生效的时间范围。
策略应用对象	目前策略应用对象有四种:基于主机 名, IP 组,用户组,和工作组。
创建状态	全局管理员创建的规则,创建状态为全 局。本地管理员创建的规则,创建状态 为本地。
创建者	此处为创建者的名称。

#### Hotfix:

当你对下载后的补丁发布后,就会在此看到相应的系统补丁,并 可对指定的补丁应用到相应的策略组,接收到此规则的终端将强 制要求安装这些系统补丁。

下载补丁操作请参照"补丁管理"



Service Pack	Hotfix
系统补丁	
策略名称	
策略描述	
选择补丁	- 
生效时间	补丁名称 补丁类型 安全公告 补丁描述 等級 发布日期 酬除 ● 所有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段
	开始时间 结束时间 编辑 副
	2012-03-10 9:00 2012-03-10 13:30 茶種
在线模式	团在线时生效团高线时生效
策略应用对象	《还没有应用到任何对象》 <u>宣看及编辑</u>
创建类型	全局
创建者	jing
注:右边有*号的项	泪必须输入。
	保存 取消

## 1.1.1. 配置要点

- 1. 点击 "ServicePack" 标签, 并点击 "添加" 按钮
- 2. 输入"ServicePack 名称"为 XP SP3
- 3. "选择操作系统"为 windows XP
- "ServicePack 主编号"选择 SP3, "ServicePack 副编号"不选
- 5. "简体中文下载网址"输入 AutoUpdate/XP/winXP-SP3.exe
- 6. "在线模式"选择为在线时生效
- 点击"策略应用对象"的"查看及编辑"按钮,选择 IP 组 类型及终端,点击"确定"
- 8. 点击"保存"进行策略保存
- 9. 点击"hotfix"标签,补丁名栏输入 KB837001 并添加
- 10. 点击"策略应用对象"的"查看及编辑"按钮,选择 IP 组类型及终端,点击"确定"
- 11. 客户端必须安装 XP SP3, 且必须安装 KB837001 这个补丁。



# 5.3. 进程运行策略

## 5.3.1. 配置介绍

此处配置可限制客户端运行的进程,比如哪些进程必须运行(红 名单),哪些进程禁止运行(黑名单),以及终端只能运行的进程 清单(白名单)。

#### 红名单

进程红名单					
NEAD					
NEEd		140			
<b>MENA</b>	主要の方法になっておけてある中国	EP-THE DANKS	/886日:再一走现行员。	and the second second	18/58
	AWER	19.84		N2(21)	112
	la contra de la co			从现本计算	ill be
在在16日11年1月4日	1 1/38				
1.100100	· MARIA CIRRAR CRIME	A CRIMINAL			
	EL MARTINA	14.9456	155 105		
	PERSONAL DEP	-91-10 AP-W 1	1.00		
usen.t	CONTRACTOR CONTRACTOR				
aseret Nikasere	Contan Canata Carrananian	Ë			
useka Kikulante Mikate	*09113 *89113 (EERCRONGER) *****	i.			

点击"红名单"标签中的"添加"按钮

配置项:	<u>说明</u>
进程名称	填写强制运行软件的进程名,如瑞星防 病毒软件的Ravmond.exe或Ravmon.exe。
下载地址	该软件的地址链接,当终端没有安装此 软件时,可通过此链接下载安装。此地 址为相对地址,如果下载的全路径为 <u>http://服务器地</u> <u>址:8833/download/software/abc.exe</u> , 则只需填写 software/abc.exe。前面的



	部分将由系统自动补充。请参考" <b>管理</b>
	网段"的"下载服务器地址"中的说明。
	可以支持完整的 url, 例如将用户现有的
	杀毒软件 url 输入即可。
	为防止恶意用户更改程序名逃避红名单
MD5 校验码	检查,可在此处填写 MD5 校验码, MD5 码
	产生工具在本系统的安装包中。
进程延迟检测时间	设置检测红名单进程的延迟时间
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种:基于主机名,
	IP 组,用户组,和工作组。

#### 黑名单

点击"黑名单"标签中的"添加"按钮



红名单 黑名单	白名单	
策略之称		
策略描述	A	
	-	
进程列表	本策略禁止终端运行以下列表中的进程。	
	世在名称 编辑	
源又件列表	本策略禁止终端运行源又伴名与以下面列表中的值匹酉的进程 资文件名	
	· · · · · · · · · · · · · · · · · · ·	
MD5码列表	本策略禁止终端运行和5码与以下列表中的值匹西的讲程	
	MD5码 编辑	
	从样本计算 添加	
动作	提示 💌	
生效时间	◎ 所有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段	
	一开始时间 结束时间 编辑 删	涂
	2012-03-10 9:00 2012-03-10 13:30 添加	
+.4×1#		
住线模式	🗹 在线时生效 🗹 离线时生效	
策略应用对象	(还没有应用到任何对象) 查 <u>看及编辑</u>	
创建类型	全局	
创建者	jing	
注: 右边有*号的项目必	·须输入。	
	保存取消	

配置项:	<u>说明</u>
进程名称	在此添加程序的进程名,如"qq.exe";
	或者其调用的 DLL 文件,如
	"QQBaseClassInDll.dll"。进程调用
	的 DLL 可从其安装目录查看,或使用专
	用工具查看。
	添加程序的源文件名,可在程序的属性,
源文件名	里面的详细信息看到,或使用专业的工
	具查看。
-+ <i>I</i> /-	在黑名单进程运行时,可选择主动的"结
	束进程",或"提示"用户,由用户自
ANTE .	行去关闭该进程。只有关闭了此进程才
	满足安全策略。



	为防止恶意用户更改程序名逃避黑名单
MD5 校验码	检查,可在此处填写 MD5 校验码, MD5 码
	产生工具在本系统的安装包中。
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种:基于主机名,
	IP 组,用户组,和工作组。

## 白名单

点击"白名单"标签的"添加"按钮

1189 289	64#	
建程白名单		
HEAR		
NOT THE OWNER		
\$1.5:552		
8183/8	RM09881 AR4888.418	
		Attata 20
105554401	8-26010231025. N. BUX	
12701A	* MARIE O INTE O #INTER O GTATER	
在铁煤式	Paulotan Paulotan	
REAL	(建築和四明時任何利用) 電道,以回動	
19842	28	
1688	area	
E DUM-RINAR	() 766.)- (20.0) (81.0)	

配置项:	<u>说明</u>
进程名称	填写此列表的名称。如"qq. exe"。
操作系统版本	选择相应的系统版本, "如 WINDOWS XP"。
非白名单进程动作	对于不在此列表内的进程的默认操作。选择 "提示"时,需要手工结束进程。选择"结 束进程"时,系统将自动终止非白单进程的 运行。注意:请谨慎使用"结束进程"选项, 以免系统将一些不在白名单上的重要的操作 系统进程终止,导致Windows不能正常工作。
MD5 校验码	为防止恶意用户更改程序名逃避黑名单检 查,可在此处填写 MD5 校验码, MD5 码产生



	工具在本系统的安装包中。
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种:基于主机名, IP
	组,用户组,和工作组。

"保存"后,点击创建好的白名单策略名称,点击"从终端取样

#### 添加"

终端IP地址:	10.201.222.44	从终端取样添加
终端取样查问	间结果	
保存选择的	项目保存所有的项目关	É
🔳 进程名科	<b>你</b>	
smss.exe	e	
csrss.ex	xe	
winlogor	n. exe	
services	s. exe	
📄 lsass.ex	xe	
vmacthly	p. exe	
svchost.	. exe	
svchost.	. exe	
svchost.	. exe	
svchost.	. exe	
svchost.	. exe	
explorer	r.exe	
spoolsv.	. exe	
VMwareTr	ray. exe	
📄 VMwareUs	ser.exe	
ctfmon.	exe	
vmtools	d. exe	

这时将会到所输 IP 的系统中将正在运行的进程以列表形式展现 出来,选择相应的进程,点击"保存选择的项目",这个进程就 被加入到白名单列表中。



注意: 白名单策略已经在进程内部将 windows 的系统进程 (c:\windows 目录下的文件)以及天珣自身的文件和进程排除 掉,因此在添加白名单进程时可忽略这些进程。

## 5.4. 软件安装策略

## 5.4.1. 配置介绍

软件安装管理可以制定软件安装的红、黑、白名单,确定用户客 户端必须安装的软件,禁止非法安装未经许可的应用软件,规定 只能安装的软件清单。

#### 软件红名单(必须安装的软件)

点击"**软件红名单"**标签中的"添加"按钮

<u>红名单</u> 黑名单	白名单文件规范
软件红名单	
策略名称	*
策略描述	
软件列表	本策略要求终端必须安装以下软件中的至少一个软件。 软件名称 下载地址 匹配方式 编辑 删除
生效时间	● 所有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段 开始时间   生作时间 ◎ は下时间段           9         所有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段           9         2012-03-10         3:30
在线模式	<ul> <li>☑ 在线时生效</li> <li>☑ 在线时生效</li> <li>☑ 高线时生效</li> </ul>
軍略应用対象 1 创建类型	(立次有应用到任何对象) 宣查必要握 全局
创建者	jing
注:右边有*号的项目必须	5输入。 保存 取消
配置项:	<u>说明</u>
策略名称	填写此软件安装策略的名称,如"必须 安装防病毒软件"



软件名称	填写必须安装的软件名称,如"瑞星" (支持模糊匹配,在控制面板中的增加 删除程序中查找匹配名称)
匹配方式	配置上面所填的软件名称是精确匹配还 是模糊匹配(在控制面板中的增加删除 程序中查找匹配名称)
下载地址	该软件的地址链接,当终端没有安装此 软件时,可通过此链接下载安装。此地 址为相对地址,如果下载的全路径为 <u>http://服务器地</u> <u>址:8833/download/software/abc.exe</u> , 则只需填写 software/abc.exe。前面的 部分将由系统自动补充。请参考"管理 网段"的"下载服务器地址"中的说明。 可以支持完整的 url,例如将用户现有的 杀毒软件 url 输入即可。
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种:基于主机名, IP组,用户组,和工作组。

### 软件黑名单 (禁止安装的软件)

点击"**软件黑名单**"标签中的"添加"按钮



红名单 黑名单	白名单	文件规范
软件黑名单		
策略名称		*
策略描述		~
软件列表	本策略禁止终端 软件名	#安装以下列表中的软件。 森 卸载参数 匹配方式 编辑 删除 模糊匹配 ▼ 添加
动作	提示	
生效时间	● 所有时间 开始 2012-03-1	◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段 和时间 结束时间 编辑 删除 10 9:00 2012-03-10 13:30 添加
在线模式	🔽 在线时生效	2 图 离线时生效
策略应用对象	(还没有应用到	到任何对象) <u>查看及编辑</u>
创建类型	全局	
创建者	jing	
注: 右边有*号的项目必	须输入。 保存 取消	
配置项:		<u>说明</u>
策略名称		填写此软件安装策略的名称,如"禁止 安装 QQ"
软件名称		填写禁止安装的软件名称,如"QQ"(支 持模糊匹配,在控制面板中的增加删除 程序中查找匹配名称)
匹配方式		配置上面所填的软件名称是精确匹配还 是模糊匹配(在控制面板中的增加删除 程序中查找匹配名称)
动作		配置当不满足此策略时客户端所发生的 动作(提示、仅记录、拦截和卸载)
生效时间		设置策略生效的时间
在线模式		配置此策略在在线和离线时是否生效
策略应用对象		目前策略应用对象有四种:基于主机名, IP组,用户组,和工作组。



### 软件白名单 (只能安装的软件清单)

点击"**软件白名单**"标签中的"**添加**"按钮

红名单 黑名单	<u>白名单</u> 文件规范
软件白名单	
策略名称	*
策略描述	
操作系统版本	₩indows 2000(32位)
软件列表	终端IP地址:
	软件名称 卸载参数 匹配方式 编辑 删除 模糊匹配 ▼ 添加
非白名单软件动作	提示
生效时间	<ul> <li>● 所有时间 ○ 1作时间 ○ 非工作时间 ○ 以下时间段</li> <li>开始时间 ○ 非工作时间 ○ 以下时间段</li> <li>2012-03-10 9:00</li> <li>2012-03-10 13:30</li> <li>添加</li> </ul>
在线模式	🗹 在线时生效 🗹 离线时生效
策略应用对象	(还没有应用到任何对象) 查看及编辑
创建类型	全局
创建者	jing
注: 右边有*号的项目必须	页输入。 【保存】 取消

配置项:	<u>说明</u>
策略名称	填写此软件安装策略的名称,如"部门 只能安装的软件清单"
软件名称	填写白名单名称(支持模糊匹配,在控制面板中的增加删除程序中查找匹配名称)
卸载参数	
匹配方式	配置上面所填的名称是精确匹配还是模 糊匹配(在控制面板中的增加删除程序 中查找匹配名称)
操作系统版本	配置此白名单软件所适用的操作系统
非白名单软件动作	配置对非白名单软件,客户端所采取的



	动作(提示、仅记录、拦截和卸载)	
生效时间	设置策略生效的时间	
在线模式	配置此策略在在线和离线时是否生效	
策略应用对象	目前策略应用对象有四种:基于主机名,	
	IP 组,用户组,和工作组。	

在"终端 IP 地址"栏中输入需要取样的终端 IP 地址, 然后点"从 终端取样添加", 这时将会到所输 IP 的系统中将已安装的软件以 列表形式展现出来, 选择相应的软件, 点击"保存选择的项目", 这个进程就被加入到软件安装白名单列表中。

终端IP地址: 10.201.222.44	从终端取样添加	
终端取样查询结果 保存选择的项目 保存所有的项目 身 ■ 软件名称	€JJ	
🔲 VMware Tools		
WebFldrs XP		
WinPcap 4.1.1		
🔲 WinRAR 压缩文件管理器		
🕅 Wireshark 1.3.3		
🔲 饊游浏览器 3		
🔲 天珣内网安全风险管理与审计系统客户	响湍	
1		

### 文件规范

点击"**文件规范**"标签中的"添加"按钮



红名单 黑名单	白名单	文件规范	
文件规范			
服用名称	· · · · · · · · · · · · · · · · · · ·		
論範擬述			
		+	
文件列表	如无 <b>张进行依本检测。则不用诸写文件版本语。</b> 文件新经 文件名称 文件版本 闭归题系 编辑 網路		
生物时间	a scenic O TA		
	Hinnin O Li	结束时间 情情 mbs	
	2012-03-10 91	00 2012-03-11 13r30	
在线模式	图 在线时生效 图 產	制度性效	
論範应用对象	《还没有应用到任何	対象) 東西辺道道	
06###	全局		
的建者	jing		
注: 古边有•号的项目必	(須輸入。 保存 取消		
配置项:		<u>说明</u>	
haden and the state of the		填写此软件安装策略的名称,如"部门	
策略名称		只能安装的软件清单"	
文件路径		填写文件存放的路径,例如C:\windows	
文件名称		填写文件的名称	
文件版本		填写文件的版本	
递归搜索		配置递归搜索(启用或不启用)	
生效时间		设置策略生效的时间	
在线模式		配置此策略在在线和离线时是否生效	
策略应用对象		目前策略应用对象有四种:基干主机名.	
		IP 组,用户组,和工作组。	

# 5.5. Windows 服务管理

5.5.1. 配置介绍

Windows 服务管理能够对用户客户端的服务进行启用、禁用管理;



对于已经启用的服务可以通过策略使其禁用,对于已经禁用的服 务也可以配置相应的策略使其启用。需要注意一点,具有依存关 系的两个服务或者是多个服务,若要禁用或启用其中的一个时, 必须同时配置其他服务的禁用和启用,策略才能生效。

## Windows 服务策略

点击 "Windows 服	务管理"页面中的	"添加"按钮	
<u>Windows服务</u>	SNMP服务		
Windows服务管理			
策略名称		*	
策略描述		×	
服务列表	服务名称	动作	编辑 删除
		禁用	▼ 添加
生效时间	🧕 所有时间 🔘 工作时间 🔘	非工作时间 🔘 以下时间	段
	开始时间	结束时间	编辑 删除
	2012-03-10 9:00	2012-03-10 13:30	) 添加
在线模式	🗹 在线时生效 🗹 离线时生效	¢	
策略应用对象	(还没有应用到任何对象)	皆看及编辑	
创建类型	全局		
创建者	jing		
注: 右边有*号的项目必须	页输入。 【保存】 取消		

配置项:	<u>说明</u>
策略名称	填写此 Windows 服务管理策略的名称, 如"管理服务"
策略描述	对该策略进行描述,便于理解
服务名称	填写服务名称
动作	选择需要启用或是禁用服务
生效时间	设置策略生效的时间
在线模式	配置策略在线或离线生效



쑢呶於田과色	目前策略应用对象有四种:基于主机名,
東哈应用刈家	IP 组,用户组,和工作组。

## SNMP 服务

点击 "SNMP 服务管理"页面中的"添加"按钮

Windows服务	SNMP服务
SNMP服务管理	
策略名称	*
策略描述	A 
动作	● 不配置 ◎ 禁用 ◎ 启用
设置默认Community String	
生效时间	◎ 所有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段
	开始时间 结束时间 编辑 删除
	2012-03-10 9:00 2012-03-10 13:30 添加
在线模式	☑ 在线时生效 ☑ 离线时生效
策略应用对象	(还没有应用到任何对象) 查看及编辑
创建类型	全局
创建者	jing
注: 右边有*号的项目必须	页输入。 【保存】 取消

配置项:	<u>说明</u>
策略名称	填写此 SNMP 服务管理策略的名称,如"管 理服务"
策略描述	对该策略进行描述,便于理解
设置默认 Community String	填写 public 或 private
动作	选择需要启用或是禁用服务
生效时间	设置策略生效的时间
在线模式	配置策略在线或离线生效
策略应用对象	目前策略应用对象有四种:基于主机名,



# 5.6. 防病毒软件策略

## 5.6.1. 配置介绍

防病毒软件策略可以控制流行的防病毒软件的程序版本和病毒 码版本。目前系统已经支持 Symantec、趋势防病毒(OfficeScan, ServerProtect)、McAfee、瑞星防病毒、微软防病毒等的版本控 制。

如果要强制终端防病毒软件的病毒库版本更新到最新版本时,需 在此设定病毒库的强制更新策略。如果要对防病毒软件的程序版 本进行管理,请使用进程管理。

#### 点击"添加"按钮配置防病毒软件策略

領職名称		•
用略描述		*
防病毒软件类型	请法择防病毒软件类	1 <b>.</b>
防病毒软件进程	同一进程可以指定多个的	856码。用分号隔开
	2,11,619	从将本计算 添加
是程虹迟检测时间	1	分钟
是否检查病毒问题本	*20g	
要求的病毒研鑽本		选择病毒药版本
病毒码延迟更新的最长天 教		00为不赚制)只有当病毒问题本高足的时候才起作用
病審码升级网址		
生物时间	■ 新有时间 ◎ 工作时	间 〇 非工作时间 〇 以下时间段
	非动物理	结束时间 编辑 删除
	2012-03-10 0:00	2012-63-10 10:30
在线模式	图在组时生效 图 南线	时生效
開略应用対象	(过没有应用到任何对象	(金) 查查及指述
创建类型	余興	
012 <b>4</b>	jing	
注:右边有•号89页目必须	isiλ.	
	保存 取消	



防病毒软件名称	输入名称如"瑞星防病毒"	
防病毒软件类型	选择相应的防病毒厂商,如"瑞星防病毒"。	
MD5 校验码	为防止恶意用户更改程序名逃避黑名单检查,可在此处填写 MD5 校验码, MD5 码产生工具在本系统的安装包中。	
是否检查病毒码版 本	默认为" <b>是</b> ";当不检查时,可选择" <b>否"</b> 。	
要求的病毒码版本	按照后面的提示,依照正确的格式输入最新的 病毒码版本,如"20.49.12"。	
病毒码延迟更新的	最后一次更新病毒码距离今天的天数,如果超	
最长天数	过了这个设定值,则被认为安全基线不合格。	
病毒码升级网址	对于提供可下载更新包的防病毒软件,可通过 此链接下载更新。此地址可填相对地址和绝对 地址,如果下载的全路径为 <u>http://服务器地</u> <u>址:8833/download/software/abc.exe</u> ,则可只 填写 software/abc.exe,前面的部分将由系统 自动补充。请参考"管理网段"的"下载服务 器地址"中的说明。	
生效时间	设置策略生效的时间	
在线模式	配置此策略在在线和离线时是否生效	
策略应用对象	目前策略应用对象有四种:基于主机名, IP 组, 用户组,和工作组。	

**注意**: 病毒码延迟更新的最长天数必须在客户端病毒码符合要求 的病毒码版本的基础上才能生效。

点击"选择病毒码版本",如果不想每次手工更新病毒码版本,



可使用此功能自动获取最新的相应的病毒码版本,自动更新的病毒码版本需要从在线补丁源中更新,随补丁更新至中心服务器。

🥶 添加病毒码版本 - Windo	ws Internet Explorer		- C ×
Attp://10.201.1.204:883	3/showViruscode.aspx?AntiV	firusName=%c8%f0%d0%	c7%c9%b1%b6%b
防病毒软件类型: 瑞星杀	毒软件		
防病毒软件版本	病毒码版本	发布时间	选择
瑞星防病毒	22, 49, 00, 01	2010-06-04	<u>选择</u>
瑞星防病毒	23. 00. 52. 12	2012-02-01	选择
瑞星防病毒	23. 00. 51. 34	2012-01-17	选择
瑞星杀毒软件	23.00.51.34	2012-01-17	<u> </u>

选定病毒码版本后,点击"选择"按钮,选择的病毒码版本将会显示在"**要求的病毒码版本**"栏中。

# 5.7. windows 账户策略

## 5.7.1. 配置介绍

Windows 账户策略是设置针对操作系统账户、密码所采取的一些加强系统安全性的策略,例如设置 windows 管理员、guest 账号, 密码复杂度和长度, 管理员权限回收等等。

账户策略

点击"账户策略"中的"添加"



帐户策略 1988年 1988년2	
新版名称 新版提述	
頭動描述	
Gaesting	● 不敢置 ○ 加用 ○ 直用
Finders管理员等号	<ul> <li>不配置</li> <li>第用内置重接负体号</li> <li>第用所有属于暂接负体号</li> <li>高用内置管接负体号</li> <li>自用所有属于管接负体号</li> <li>自用所有属于管接负相关等</li> </ul>
Nadaes管理员缺省转号 之间	we want the second s
新户版室	118:3 A 2012年11月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日
同户积限分离	次元防量単立協改業内:特内的設計詞: 分钟,在 分钟后期位帐户防空计数器 ● 不適用 ● 为用户地址加減员 ● 走加新用户期间制作不在列表中的用户组成员
¥周七朝秋天周秋户	注意: 如果許讓不存在新聞的調中或用戶语,系统將不会自动就證。多1條戶用/稿并。 「不說意 ○ 疑用 ○ 歸解
·····································	意:在上集中的"他户科建国用或制作。不会制作系统内面的"他户。 和高制作用新量学们用户,等时不定量未无法注入系统,请安全使用。 20
E2981A a	- 新和时间 〇 工作时间 〇 以下时间的 - 川山町は
	2012-03-03 8:00 2012-03-10 13:30 200
EXEMPT 1	2012-03-00 8:00 2012-03-10 13:30 2012-03-10 13:30 2012-03-00
目接續式 )。 前配位用对象 (	2012-03-09 8:00 [2012-03-10 13:30 ] [2010-03 [在6時1主政 [2] 展6時1主政 译沒與成用對任何対象) 重点Z:[2]]
1235項式 [] 前配位用対象 ( 1388本型 全	2012-03-00 8:00 2012-03-10 13:30 2012-03-0 7在5時1主政 20 高5時1主政 建設集成用制任何対象) 素素及2500 局
在15項式 () 1988年月11世 ( 1988年年初 全 1988年 ()	2012-03-08 8:00 2012-03-10 13:30 2012-03-10 2012-03-100-10 13:30 2012-03-100-10-10-10-10-10-10-10-10-10-10-10-10

配置项:	<u>说明</u>
策略名称	输入加固策略的名称,如"加固策略-财务部"。
Guest 账号	可以选择启用或禁用 guest (来宾) 账号, 注: 取消"禁用"后, 需配置"启用"才会启用 guest 账号。
Windows 管理员账号	可启用或禁用内置管理员或属于管理员组的账 号
Windows 缺省管理员账号	修改管理员缺省帐号名称,默认缺省值为 Administrator。

Ţ



账户锁定	发生无效登录后锁定使用的登录账户
用户权限分离	为 windows 用户组添加成员或移除某些不在用 户组的成员
禁用和删除无用账户	可以删除或者禁用非 windows 内置账户,注: 可能会删除当前登录的用户,导致下次登录无 法进入系统,请安全使用。
策略执行周期	设置执行本条策略的周期时间。注:只能是5 或者5的倍数。
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种:基于主机名, IP 组, 用户组,和工作组。

### 密码策略

密码策略可以对 windows 密码长度,复杂度和使用时间进行配置 更改,以达到保护系统的效果。

点击"密码策略"中的"添加"



液码管路				
10 19 34 40				
崔峰名称				
解释描述				
密码必须符合复杂性要求	● <b>不能置</b> ○ MR ○ £	ід		
密码长度最小值		带带+		
密码最长使用期间		失•		
重码最短使用期限		天*		
運動密码防史	● 不配置 ○ 取消援制密码历史			
	◎ 保留密码历史	个记住的密码		
部最执行周期	3600	-W		
生效时间	• 所有时间 〇 工作时)	a○ #I@时间○	大时间段	
	2012-00-10 Pros	2012-03-10	13130	15 Fel .
在线模式	Names & Rad	19.00		
副郵应用対象	(还没有应用到任何对象	) 重要应用机		
创建类型	<b>金</b> 局			

配置项:	<u>说明</u>
策略名称	输入策略名称。
密码必须符合复杂性要求	本地策略中启用或禁用密码复杂度
密码长度最小值	可以将值设置为介于 1 和 14 个字符 之间,或者将字符数设置为 0 以确定不 需要密码。
密码最长使用期限	可以将密码设置为在某些天数(介于 1 到 999 之间)后到期,或者将天数设置 为 0,指定密码永不过期。安全最佳操 作是将密码设置为 30 到 90 天后过 期,密码最长使用期限不超过 999 天。
密码最短使用期限	密码最短使用期限必须小于密码最长使 用期限,除非将密码最长使用期限设置 为 0,指明密码永不过期。如果将密码 最长使用期限设置为 0,则可以将密码





	最短使用期限设置为介于 0 和 998 之	
	间的任何值。	
强制密码历史	此安全设置确定再次使用某个旧密码之	
	前必须与某个用户帐户关联的唯一新密	
	码数。该值必须介于 0 个和 24 个密码	
	之间。	
策略执行周期	默认为 3600 秒, 且无法修改	
生效时间	设置策略生效的时间	
在线模式	配置此策略在在线和离线时是否生效	
策略应用对象	目前策略应用对象有四种:基于主机名,	
	IP 组,用户组,和工作组。	

#### 管理员权限回收

对注册表的某些项进行保护,以此来防止某些非法程序对注册表 进行非法的修改。

#### 点击"管理员权限回收"标签中的"添加"按钮

帐户策略 密码第	短略 <u>管理员权限回收</u>
管理员权限回收	
策略名称	*
策略描述	*
	-
注: 配置有安全基线密码	马策略时,帐号权限回收策略无效
管理员帐号	*
密码	显示明文
生效时间	◉ 所有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段
	开始时间 结束时间 编辑 删除
	2012-03-10 9:00 2012-03-10 13:30 <b>添加</b>
在线模式	🗹 在线时生效 🗹 离线时生效
策略应用对象	(还没有应用到任何对象) 查看及编辑
创建类型	全局
创建者	jing
注: 右边有*号的项目必	须输入。 【保存】取消



配置项:	<u>说明</u>
策略名称	输入注册表保护策略的名称。
描述	该策略的详细说明
管理员账号	设置 windows 新的管理员账号,并把 administrator 账号禁用和生成一个
	cebuser 普通用户账户。
密码	设置 windows 新的管理员账号密码
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种:基于主机名, IP组,用户组,和工作组。

# **5.8.** Windows 本地策略

5.8.1. 配置介绍

审核策略

点击"**审核策略**"中的"添加"



<u>审核策略</u> 用户权	限分配 安全选项 IP协议安全 数据执行保护
策略名称	*
策略描述	A
审核所选项目操作	
	◎ 不配置 ◎ 审核过程(进程)追踪 □ 成功 □ 失败
	◎ 不配置 ◎ 审核目录服务访问 🛛 🗍 成功 🗌 失败
	◎ 不配置 ◎ 审核特权使用
	◎ 不配置 ◎ 审核系统事件
	◎ 不配置 ◎ 审核帐户登录事件 □ 成功 □ 失败
<b>坐</b> 廠协行 国期	
\$\$\$\$\$\$\$\$\$\$\$\$\$\$	3600 #2
王双时间	
	77.第四回 36.74回 3冊項 明际 2012-03-10 9.00 2012-03-10 13.30 天地
	2012-03-10 9:00
在线模式	🗹 在线时生效 🔽 离线时生效
策略应用对象	(还没有应用到任何对象) 查看及编辑
创建类型	全局
Ant	
创建者	jing
注: 右边有*号的项目必	页输入。 【保存】取消
· 町里西	24 00
阳且坝:	<u> </u>
策略名称	输入策略的名称。
·# \-	<u></u>

该策略的详细说明
设置审核策略的类型和动作,可选择"成 功"与"失败",或全部选择。
默认为 3600 秒并不能修改
设置策略生效的时间
配置此策略在在线和离线时是否生效
目前策略应用对象有四种:基于主机名, IP组,用户组,和工作组。

## 用户权限分配

点击"用户权限分配"中的"添加"



审核策略	<u>用户权限分配</u> 安全选项 IP协议安全 数据执行保护
用户权限分	Be.
策略名称	*
策略描述	·
用户权限分配	● 不敬署
	◎ 允许下表中的用户或用户组
	□ 远程关机
	<ul> <li>中央地关机</li> <li>取得文件或其他对象的所有权</li> </ul>
	名称 用户或用户组 编辑 删除
策略执行周期	◎ 用户组 ◎ 用户 ※加 3600 秒
生效时间	◎ 所有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段
	开始时间 结束时间 编辑 删除
	2012-03-10 9:00 2012-03-10 13:30 添加
在线模式	🗹 在线时生效 🗹 离线时生效
策略应用对象	(还没有应用到任何对象) 查看及编辑
创建类型	全局
创建者	jing
注: 右边有*号的	
	保存取消
记置项:	<u>说明</u>
宦略名称	输入策略的名称。
拔	该策略的详细说明
	名称一项中填写的用户/用户组,将赋:
古古初阳八声	一 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
了仅限分配	远在大加、
	对象的所有权的权限。
宦略执行周期	默认为 3600 秒并不能修改
E效时间	设置策略生效的时间

 在线模式
 配置此策略在在线和离线时是否生效

 策略应用对象
 目前策略应用对象有四种:基于主机名,

 IP 组,用户组,和工作组。

## 安全选项



设置针对操作系统所采取的一些加强系统安全性能的策略,例如

隐藏登录名,禁止自动播放策略等。

审核策略 用户权限	限分配 安全选项 IP协议安全 数据执行保护
安全选项	
策略名称	*
策略描述	
隐藏上次登录用户名	◎ 不配置 ◎ 禁用 ◎ 启用
关机时清理虚拟内存页面 文件	◎ 不配置 ◎ 禁用 ◎ 启用
本地帐户的共享和安全模 式	◉ 不配置 ◎ 经典 ◎ 仅来宾
自动播放	◎ 不配置 ◎ 禁用 ◎ 启用
安全模式	◎ 不配置 ◎ 禁用 ◎ 启用
策略执行周期	3600 秒
生效时间	◎ 所有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段
	开始时间 结束时间 编辑 删除
	2012-03-10 9:00 2012-03-10 13:30 添加
在线模式	🗹 在线时生效 🗹 离线时生效
策略应用对象	(还没有应用到任何对象) 查看及编辑
创建类型	全局
创建者	jing
注: 右边有*号的项目必须	·输入。 保存 取消

配置项:	<u>说明</u>
策略名称	输入加固策略的名称,如"加固策略-财务部"。
说明	该规则的详细说明
隐藏上次登录用户名	在windows9x以上的操作系统中对以前的用户 名具有记忆功能,下次重启时,在登录框中会 发现上次登录的用户名。为了避免这些信息被 非法用户利用,有必要将他隐藏起来。
关机时清理虚拟内存页面文 件	解决系统空间不足,电脑关机时清空虚拟内存 页面文件将会对系统空间进行优化
本地帐户的共享和安全模式	所谓的经典即访问共享需要输入用户名和密码 等,所谓的仅来宾即网络访问的权限仅为 everyone 权限。与 Windows 组策略中"网络访



	问:本地帐户的共享和安全模式"统一。
自动播放	即禁用光盘、USB 设备等的自动播放功能。注: 取消"禁用"后,需配置"启用"才会启用自 动播放功能
安全模式	即系统启动时无法选择下拉列表框。对于双引 导系统的电脑有影响,而且无法进入安全模式 进行问题恢复。说明:禁止进入安全模式有一 定的风险,启用这个选项要谨慎(Vista和Win 2008,Win 7 无效)。注:取消"禁用"后,需 配置"启用"才能进入安全模式。
策略执行周期	默认为 3600 秒并不能修改
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种:基于主机名, IP 组, 用户组,和工作组。

## IP 协议安全

通过加固 TCP/IP 协议栈防范,尽可能的减轻 SYN 攻击的危害



审核策略 用户权	限分配 安全选项 <u>IP协议安全</u> 数据执行保护
IP协议安全	
策略名称	*
策略描述	
是否启用SYN攻击防护	◎ 是 ◎ 否
设置触发SYN洪水攻击保 护所必须超过的TCP连接 请求阀值	0 (推荐值:5)
设置处于SYN_RCVD状态的 TCP连接数的阀值	0 (推荐值: 500)
设置处于至少已发送一次 重传的SYM_RCVD状态中的 TCP连接数的阀值	0 (推荐值: 400)
策略执行周期	5 秒
生效时间	<ul> <li>● 所有时间 ○ 工作时间 ○ 非工作时间 ○ 以下时间段</li> <li>开始时间 结束时间 编辑 删除</li> <li>2012-03-10 9:00 2012-03-10 13:30 添加</li> </ul>
在线模式	☑ 在线时生效 ☑ 离线时生效
策略应用对象	(还没有应用到任何对象) <u>查看及编辑</u>
创建类型	全局
创建者	jing
注: 右边有*号的项目必须	<sup>页输入。</sup> 保存 取消

配置项:	<u>说明</u>
策略名称	输入策略的名称。
描述	该策略的详细说明
是否启用 SYN 攻击防护	可选择开启或不启用 SYN
设置触发 SYN 洪水攻击保 护所必须超过的 TCP 连接 请求阀值	TcpMaxPortsExhausted 是指系统拒绝的 SYN 请求包的数量,默认是 5。
设置处于 SYN_RCVD 状 态的 TCP 连接数的阀值	TcpMaxHalfOpen 表示能同时处理的最 大半连接数,如果超过此值,系统认为 正处于 SYN 攻击中。 默认值为 500
设置处于至少已发送一次 重传的 SYN_RCVD 状态 中的 TCP 连接数的阀值	TcpMaxHalfOpenRetried 定义了保存在 backlog 队列且重传过的半连接数,如果 超过此值,系统自动启动



	SynAttackProtect 机制。 默认值为 400		
策略执行周期	<b>执行周期</b> 设置执行本条策略的周期时间。注:只能是5或者5的倍数。		
生效时间	设置策略生效的时间		
在线模式	<b>奠式</b> 配置此策略在在线和离线时是否生效		
策略应用对象	目前策略应用对象有四种:基于主机名, IP 组,用户组,和工作组。		

### 数据执行保护

DEP(Data Execution Prevention)即"数据执行保护",这是 Windows 的一项安全机制,主要用来防止病毒和其他安全威胁对 系统造成破坏。

审核策略 用户权	限分配 安全选项 IP协议安全 <u>数据执行保护</u>		
数据执行保护			
策略名称	*		
策略描述			
设置Windows的DEP(数据 执行保护)功能 策略执行周期	<ul> <li>● 不配置</li> <li>● 仅为基本Windows程序和服务启用DEP</li> <li>● 为所有程序和服务启用:</li> <li>注: 必须重启系统生效。</li> <li>5</li> </ul>		
生效时间	<ul> <li>● 所有时间 ○ 工作时间 ○ 非工作时间 ○ 以下时间段</li> <li>● 开始时间 ○ 非工作时间 ○ 以下时间段</li> <li>□ 2012-03-10 9:00</li> <li>□ 2012-03-10 13:30</li> <li>□ 添加</li> </ul>		
在线模式	<ul> <li>✓ 在线时生效</li> <li>✓ 离线时生效</li> <li>(还没有应用到任何对象) 查看及编辑</li> </ul>		
策略应用对象			
创建类型	全局		
创建者	jing		
注:右边有*号的项目必须输入。 保存 取消			
配置项:	<u>说明</u>		
策略名称	输入策略的名称。		
描述	该策略的详细说明		



设置 Windows 的 DEP(数 据执行保护)功能	为windows 程序和服务启用 DEP
策略执行周期	设置执行本条策略的周期时间。注:只能是5或者5的倍数。
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种:基于主机名, IP组,用户组,和工作组。

# 5.9. 注册表策略

## 5.9.1. 配置介绍

对注册表的某些项进行检测和保护,以此来防止某些非法程序对 注册表进行非法的修改。

点击"**注册表策略"**标签的"添加"



	注册表如用			
	注册表策略			
	解释名称			
	网络铁团	-	(A)	
	注册表检测	日田玉英	確認とは 確認的な法 約1000円 1995 1998 RD5_52 ・ 553g	
	注册表保护	11日A10	1993年4月,2月1日の1月1日 1月1日日 - 1月1日日日 1月1日日 - 1月1日日日 1月1日日日 - 1月1日日日 1月1日日日 - 1月1日日日 1月1日日日 - 1月1日日日 1月1日日日 - 1月1日日日 1月1日日日 - 1月1日日日 1月1日日日 - 1月1日日日 1月1日日 - 1月1日日日 1月1日日 - 1月1日日日 1月1日日 - 1月1日日 1月1日日 - 1月1日 1月1日日 - 1月1日 1月1日日 - 1月1日 1月1日日 - 1月1日 1月1日日 - 1月1日 1月1日 1月1日 - 1月1日 1月1日 1月1日 - 1月1日 1月1日 1月1日 1月1日 - 1月1日 1月1日 1月1日 - 1月1日 1月1日 1月1日 1月1日 1月1日 1月1日 1月1日 1月1日	
	# Overlid	王: 当前把武型为886。	tenuced,對据公示十进制整数。	
		12012-03-10 m00		
	在线模式	回在鄉性故 回赢的	厚沙生效	
	蒲峰位用对象	《逆及有应用到任何对	第> 重動及濃幅	
	的建杂型	全局		
	創建者	jing		
	注:有边陲*鸣的规则	但在 取消		
酉	配置项:		<u>说明</u>	
策	略名称		输入策略名称	
策	策略说明:		规则更详细的描述或说明	
			填入需要保护或检测的注册表项,如	
注册表项			"HKEY_LOCAL_MACHINE\SOFTWARE\M	
			icrosoft\Windows	
			\CurrentVersion\Run"	
			填入该注册表项下的键值名称,如	
			"RavTask",则保护该值不被修改;	
键值名称			若不填写则保护整个 run 项,该项下	
			禁止删除、更改、创建任意注册表键	
			值。	
键	值数据		填入该键准确的数据值	
			根据实际填写的键值的类型选择,	
数据类型			REG SZ 为字符串类型, REG DWORD 为	
			★刑粉党 PEC MILTI C7 与夕亏位中	
			亚空奴士,NLU_MULII_54 八多子付申	
			类型。	


生效时间	设置策略生效的时间范围			
在线横式	配置此策略在在线和离线时是否生			
	效			
等败应田对象	目前策略应用对象有四种:基于主机			
水响广工口小)家	名, IP 组, 用户组, 和工作组。			

# 5.10. 共享资源管理

## 5.10.1. 配置介绍

设定策略对终端共享资源控制和管理,此功能限制资源的随意共 享和使用。通过定制策略取消已经共享的资源,并禁止 windows 共享功能。

新局名称						
WHEN WAR						
NO-E BUCK						
共享目录活动	· 禁止设立共享回录,取消	现有所有共享并帮止	其單級件			
	允许设立共享目录,并为	指定共享目录进行用/	户授权		-	
	(包含金糖経)	2000		부모명		196 90
		1	同識取	回要改	而完全控制	清加
机变打印机铁场	便权用户可以为Iveryenes f	《法全部用户- 各个用	户之间用	18开*		
	竹祥县掌打印机					
共享IFCS通项	· ····································					
	C Train H Broot					
	小小小に計画書があ					
NAMES AND ADDRESS OF TAXABLE ADD	"加果选择不允许共享IIIC\$后	再选择代许共享IN	和探護機構	夏重高后7	才能物夏17C共同	E.
新版执行规则 + 365-62	"加限选择不允许共要Inci后 5	,再选择光讲共享170 砂	1013SMR	價重自后?	対影物変いて共同	r.
解释执行周期 生效时间	● 新有时间 ● 工作时间 ●	・ 再选择共享共立 8 第二作时间 〇 以下	an faise an de Internation	便重点后?	<b>计能协变</b> 1854年度	r.
新聞执行周期 主效时间	*小田支援不大計共業Incs長 5 ● 新有时间 ○ 工作时间 ○ 月前日日	- <b>再迭時代決共享の</b> 9 日本11年1月 〇 以下 11月11月 〇 以下 11月11月	no postanta et indeg	<b>要重点后</b> 。 1955		r
解關执行風期 主效时间	*加減速不死計共業Incs長 5 ● 新有时间 ○ 工作时间 ○ 月 ○日11 2012-09-10 9:00	<ul> <li>再选择代算共享中で</li> <li>移</li> <li>第工作时间 〇 以下</li> <li>第工作时间 〇 以下</li> <li>(2012-07-01-1</li> </ul>	HER FRANK	<b>要重点后</b> 。 编成		r
葡萄执行周期 主效时间 在纸模式	* 新有时间 ○ 工作时间 ○ 第一回 「「」」 ● 新有时间 ○ 工作时间 ○ 1 ○ 1 ○ 1 □ 1 □ ○ 1 ○ 1 □ □ 1 □ 1 □ ○ 1 ○ 1 □ 1 □ 1 □ 1 □ ○ 1 ○ 1 □ 1 □ 1 □ 1 □ 1 □ 1 □ 1 □ 1 □ 1	<ul> <li>         ・ 再送信代計共専         ・ (株式)         ・ (株式)         ・         ・         ・</li></ul>	NATES OF CONTRACTS			r
新時共行周期 主効时间 在紙欄式 解明の用対象		<ul> <li>         ・ 再述指分法共変のの ・ 教工作时间 〇 以下 ・ 外立でけ ・ ハンマリコ         ・ ハンマリコ         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	an a			r.
新時共行周期 主効时间 在线模式 新時の用対象	* 日本語名で大計 共業100名 * 日本語名で大計 共業100名 5 ● 新有时间 ○ 工作时间 ○ 12012-05-009-00 「2012-05-009-00 「2012-05-009-00 「2012-05-009-00 「2012-05-009-00 「2012-05-009-00 」 2012-05-009-00 「2012-05-009-00 」 2012-05-009-00 「2012-05-009-00 」 2012-05-009-00 「2012-05-009-00 」 2012-05-009-00 「2012-05-009-00 」 2012-05-009-00 「2012-05-009-00 」 2012-05-009-00 「2012-05-009-00 」 2012-05-00 「2012-05-009-00 」 2012-05-00 「2012-05-009-00 「2012-05-00 」 2012-05-00 「2012-05-00 」 2012-05-00 「2012-05-00 「2012-05-00 」 2012-05-00 「2012-05-00	<ul> <li>         ・ 再送信代法共変のの         ・         ・         ・</li></ul>	和於國際 时间限 Janao			E.
新聞执行周期 主効时间 在球機式 新聞忍用対象 80種类型	***********************************	<ul> <li>         ・用述指允许共変のの         ・         ・         ・</li></ul>	和代码。 时间积 3130	<b>要业</b> 此后7 1953		E.
新聞执行周期 主効时间 在近機式 新聞の用対象 8月建夫型 10月建夫型	***********************************	<ul> <li>         ・用述指示法共変の         ・         ・         ・</li></ul>	at Alag	<b>要重点后</b> 。		
新聞执行周期 主动时间 在北線式 新聞の用対象 6月建夫型 日曜為 主:右边有+号的项目	***********************************	<ul> <li>         ・用述指示法共変の         ・         ・         ・</li></ul>	和1999年(1999年) 日本日本日 1999年) 1999年)	<b>曹重此后</b> 7 [4]第 [1] [1]		E
新聞执行開期 主动时间 在紀復式 前間の用対象 80歳実型 回復者 注:右边有+号的项目	10日東京市大計具第10日 10日東京市大計具第10日 5 ※ 所有时间 〇 工作时间 〇 2010年1日 年1日 2010年1日 年1日 2010年11日 2010年11111111111111111111	<ul> <li>         ・用述指示法共変のの         ・         ・         ・</li></ul>	AD (1993) At IRAN State			E
新聞执行開期 主动时间 在北線式 新聞の用対象 80歳夫型 回還者 注:右边有+号的页	***********************************	<ul> <li>         ・用述指示法共変の         ・         ・         ・</li></ul>	10 (19 14 16 16 16 16 16 16 16 16 16 16 16 16 16			

点击"**共享资源策略**"的"添加"



策略名称	输入策略名称		
策略说明:	规则更详细的描述或说明		
	配置允许共享、不允许设立共享(已		
	经共享的目求会被取消),选择允许 设立共享目录,在共享录名可填写路		
共享目录选项	径如:C:\windows\share,授权用户		
	可填写用户名如: Administrator,		
	共享权限可组合选择"读取、更改和		
	完全选择三项"		
ᄮᆃᆄᇭᆁᄽᆓ	配置允许共享打印机、不允许共享打		
<del>八</del> 季打印机选坝	印机		
	配置允许共享 IPC\$、不允许共享		
	IPC\$,选择不允许共享 IPC\$后,再		
关子 IFC9	选择允许共享 IPC\$时终端需要重启		
	后才能恢复 IPC 共享		
쇼 my ᅯ, 仁 田 바미	设置执行本条策略的周期时间。注:		
東哈與行向别	只能是5或者5的倍数。		
生效时间	设置策略生效的时间		
<b>左</b> 华 博 子	配置此策略在线和离线是否生效。此		
江线侠风	处默认在线离线都生效		
策略应用对象	目前策略应用对象有四种:基于主机 名, IP 组,用户组,和工作组。		

# **5.11.** Windows 事件日志管理策略

# 5.11.1 配置介绍

可以通过配置 Windows 事件日志管理策略,管理 windows 应用



程序、安全、系统日志文件大小,可对系统的各项操作有更全面、

更长久的详细了解

点击"Windows 事件日志管理"的 "添加"

Windows事件日志管理	
策略名称	*
策略描述	*
	-
Windows事件日志最大日 志文件大小	□ 应用程序KB
	注:如果您的系统是win7,应用程序、安全、系统、这三项的输入的最小值应是1024
当Windows事件日志达到 最大的日志大小时	◎ 按需要覆盖事件(旧事件优先)
	◎ 当操作系统版本为Vista及以上版本时,日志满时将其存档,不覆盖事件;当操作系统为XP或2003时,存档或改写
	改写久于 天的事件
	◎ 不覆盖事件(手动清除日志)
策略执行周期	5 秒
生效时间	◎ 所有时间 🛇 工作时间 🛇 非工作时间 🛇 以下时间段
	开始时间 结束时间 编辑 删除
	2012-03-10 9:00 2012-03-10 13:30 添加
在线模式	☑ 在线时生效 ☑ 离线时生效
策略应用对象	(还没有应用到任何对象) 查看及编辑
创建类型	全局
创建者	jing
注: 右边有*号的项目必须	须输入。 【保存】 取消

配置项:	<u>说明</u>
策略名称	输入策略名称
策略描述:	规则更详细的描述或说明
Windows 事件日志最大日 志文件大小	设置应用程序、安全、系统的日志文 件大小,最小值为1024
当 Windows 事件日志达到 最大的日志大小时	当 Windows 事件日志达到最大的日 志大小时,可选择自动覆盖旧事件或 手动清除旧日志文件
策略执行周期	设置执行本条策略的周期时间。注: 只能是5或者5的倍数。

生效时间	设置策略生效的时间段
在线模式	配置此策略在线和离线是否生效。此 处默认在线离线都生效
策略应用对象	目前策略应用对象有四种:基于主机 名, IP组,用户组,和工作组。

# 5.12. 用户环境策略

## 5.12.1. 配置介绍

### AD 域策略

点击"AD 域策略"标签的"添加"按钮

AD域策略 屏幕保	护策略 IE配置 远程桌面管理 禁止修改网卡
AD域策略	
策略名称	*
策略描述	
域名	域名必须与终端所隶属的域名一致。
检测选项	◉ 仅需要加入域 ◎ 需要加入且登录域
是否排除XP HOME版及 win7 home版本	◎否 ◎是
生效时间	◎ 所有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段
	开始时间 结束时间 编辑 删除 2012-03-10 13:30 添加
在线模式	🗹 在线时生效 🗹 离线时生效
策略应用对象	(还没有应用到任何对象) 查 <u>看及编辑</u>
创建类型	全局
创建者	jing
注: 右边有*号的项目必须	输入。 保存 取消
配置项:	<u>说明</u>
策略名称	简单明了的策略名称
域名	终端电脑必须加入的 AD 域的名称。
检测选项	选择"是"将对终端是否加入了 Windows AD



	域进行检查。
是否排除 XP HOME 版及	选择"是"对 XP HOME 版及 win7 home 版本的
win7 home版本	操作系统不做检查。
生效时间	设置策略生效的时间段
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种:基于主机名,IP 组,用户组,和工作组。

### 屏幕保护策略

可以通过定制屏幕保护策略,使接收到策略的终端的自动启用屏 幕保护。

点击"**屏幕保护策略"**标签的"添加"

AD域策略	<b>ண (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)</b>
策略名称	*
策略描述	
	◎ 不配置 (不改变终端现有的屏保设置)
	◎ 强制启用屏保(没有设置则选择默认屏保)
	□ 启用屏保的等待时间必须小于
	□ 屏保恢复时显示登录界面
	○ 奴利毋保(自幼宗用终端毋保) □ 禁止使用欢迎界面 注:*仅限于XP或VISTA或Window7系统的客户端
	□ 辇止使用快速切换用户 注:*仅限于XP或VISTA或Window7系统的客户
策略执行周期	5 ¥b
	5 P
生效时间	◉ 所有时间 🔍 工作时间 🔍 非工作时间 🔘 以下时间段
	开始时间 结束时间 编辑
	2012-03-10 9:00 2012-03-10 13:30 添加
在线模式	🗹 在线时生效 🗹 离线时生效
策略应用对象	(还没有应用到任何对象) <u>查看及编辑</u>
创建类型	全局
创建者	jing
注:方动有*号的顶眼	
THE PROPERTY OF THE PARTY OF	
	保存 取消
	保存取消

西



策略名称	输入策略名称
策略说明:	规则更详细的描述或说明
不配置	不改变终端现有的屏幕保护设置
强制启用屏保	如果选中这个选项,如果客户端原先 没有启用屏幕保护,系统将自动启用 一个名为"空白"的屏幕保护程序。 如果选中这个选项,如果客户端原先 已经启用了屏保,系统将继续使用该 屏保 如果不选中这个选项,则保留客户端 原来的配置。
启用屏保的等待时间必须 小于…分钟	如果选中这个选项,客户端原来的屏 保时间大于这个时间时,系统将自动 把客户端的设置改为这里输入的时 间;如果客户端原来的时间小于这个 时间时,系统则保持该时间不变。 如果不选中这个选项,则保留客户端 原来的配置。
取消 屏保	选中这个选项,如果终端原先没有启 动屏保,则保持原状;如果中断原先 启用了屏保,系统将自动禁用该屏 保。
屏保恢复时显示登陆界面	如果选中这个选项,系统将自动更改 客户端设置使之与管理员设置一致。 如果不选中这个选项,则保留客户端 原来的配置。
禁止使用欢迎界面	如果选中这个选项, Windows 将不显



	示欢迎页让用户点击用户登录,而是
	要输入用户名进行登录。
	如果不选中这个选项,则保留客户端
	原来的配置。
	如果选中这个选项, Windows 将不出
林小铁田特年四秋田宁	现切换用户界面。
<u> 亲</u> 工 使 用 沃 速 切 <del>狭</del> 用 <i>广</i>	如果不选中这个选项,则保留客户端
	原来的配置。
	如果选中这个选项,当客户端
Windowa 光前终寻密如不能	Windows 当前登录用户密码为空,将
WILLOWS 当时豆水雷码个能	提示安全状态不合格。
为王	如果不选中这个选项,则不检查登录
	用户的密码是否为空。
AATTIN THE ATTIN	设置执行本条策略的周期时间。注:
東哈扒仃向别	只能是5或者5的倍数。
生效时间	设置策略生效的时间
ᄻᇔᆎᆣᄪᅶᆇ	目前策略应用对象有四种:基于主机
東略巡用灯家	名, IP 组, 用户组, 和工作组。

### IE 配置

大多安全隔离要求较高的网络会使用 WEB 代理上网。在这种模式下,需要统一设置很多配置。IE 策略可以为所有终端统一添加例外排除的配置信息,大大减轻了管理员的管理工作。

点击"IE 配置"中的"添加"



AD域策略	屏幕保护策略	<u>IE配置</u>	远程桌面管理	)
IE配置				
策略名称				*
策略描述				*
是否对所有可信: 求用https访问		否		Ŧ
将以下站点添加。 点	□□1言55			ł
将以下站点从可 移除	<b>言</b> 站点中			>>
				>>
IB代理例外列表	将以下地	址添加到工图代理例	外列表:	•
	将以下地	址从IE代理例外列	表中移除:	>>
				+
策略执行周期	5		 秒	>>
生效时间	● 所有时间 ○ 工作 开始时间           2012-03-10 9:0	<b>时间 ◎ 非工作时间 ◎</b> 结 0	以下时间段           束时间         编辑           10 13:30         湯	· 删除 动们
在线模式	🗹 在线时生效 🔽 离	线时生效		
策略应用对象	(还没有应用到任何双	<b>掾</b> ) <u>查看及编辑</u>		
创建类型	全局			
创建者	jing			
注: 右边有*号的项目必须	输入。 <b>保存</b> 取消			

配置项:	说明
策略名称	输入合适的策略名称,以方便管理。
策略描述	用以描述该 IE 代理上网的提示信息,以方便管理。



是否对所有可信站点都 要求用 https 访问	选择让 IE 使用 HTTPS 访问可信站点	
将以下站点添加为可信 站点	在此添加可信站点	
将以下站点从可信站点 中移除	在此取消可信站点	
IE 代理例外列表	输入不通过 Proxy 访问的 By Pass 主机或网段的列表	
策略执行周期	设置执行本条策略的周期时间。注: 只能是 5 或者 5 的倍数。	
生效时间	设置策略生效的时间	
策略应用对象	目前策略应用对象有四种:基于主机名, IP 组, 用户组,和工作组。	

### 远程桌面管理

通过配置远程桌面管理策略,可以阻止或允许远程计算机对本机 的远程操作动作。

AD域策略 屏幕	保护策略 IE配置 <u>远程桌面管理</u> 禁止修改网卡
远程桌面管理	
策略名称	*
策略描述	
远程桌面选项	◎ 不配置 ◎ 启用 ◎ 禁止
生效时间	<ul> <li>● 所有时间 ○ 工作时间 ○ 非工作时间 ○ 以下时间段</li> <li>开始时间   结束时间   编辑 删除</li> <li>2012-03-10 9:00   2012-03-10 13:30   添加</li> </ul>
在线模式	🗹 在纽时生效 🗹 离线时生效
策略应用对象	(还没有应用到任何对象) 查看及编辑
创建类型	全局
创建者	jing
注: 右边有*号的项目必	须输入。 【保存】 取消



配置项:	说明	
策略名称	输入策略名称	
远程桌面选项	选择本机是否开启远程桌面	
生效时间	设置策略生效的时间	
在线模式	选择该策略生效的网络场景,分为"在线时生效" 和"离线时生效"	
策略应用对象	目前策略应用对象有四种:基于主机名, IP 组, 用户组,和工作组。	

### 禁止修改网卡

点击"**禁止修改网卡"**的"添加"

禁止修改网卡功能可以防止使用人擅改网卡 IP 地址, mac 地址 等等之类的属性。

AD域策略 屏幕保	护策略 IE 配置 远程桌面管理 <u>禁止修改网卡</u>
禁止修改网卡	
策略名称	*
策略描述	
网卡属性	<ul> <li>不配置</li> <li>不位许修改</li> <li>不行许修改</li> </ul>
策略执行周期	5 秒
生效时间	◎ 所有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段
	开始时间
	2012-03-10 9:00 2012-03-10 13:30 添加
在线模式	🗹 在线时生效 🗹 离线时生效
策略应用对象	(还没有应用到任何对象) 查看及编辑
创建类型	全局
创建者	jing
注:右边有*号的项目必须	输入。
	保存 取消
配置项:	说明
策略名称	输入策略名称



网卡属性	配置是否允许修改网卡属性	
策略执行周期	设置执行本条策略的周期时间。注: 只能是 5 或 者 5 的倍数。	
生效时间	设置策略生效的时间	
在线模式	选择该策略生效的网络场景,分为"在线时生效" 和"离线时生效"	
策略应用对象	目前策略应用对象有四种:基于主机名, IP组, 用户组,和工作组。	

"发送到"菜单选项

点击""发送到"菜单选项"的"添加"

"发送到"菜单	选项			
1968名称			6	
前相任过		*		
"发送到"菜单透顶	* 782 0 88 0 M	(*) 1		
网络执行周期	5	8		
生物封阔	• NAME O LANE RECEI [2019-0-10 900	0 #100 0 0000 (0000) (0000) (00000)		
在线模式	REALED RANNI	10		
解释应用对象	(建没有应用到任何对象)	<u>267/88</u>		
が建た型	全間			
068 <b>4</b>	jing			
注: 右边有+号的项目会	(2) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1			

配置项:	说明	
策略名称	输入策略名称	
"发送到"菜单选项	配置启用或禁止 <b>"发送到"菜单选项</b>	
等败劫行周期	设置执行本条策略的周期时间。注: 只能是5或	
來咁1八11 /可为1	者5的倍数。	

T



生效时间	设置策略生效的时间
在线模式	选择该策略生效的网络场景,分为"在线时生效" 和"离线时生效"
策略应用对象	目前策略应用对象有四种:基于主机名, IP 组, 用户组,和工作组。

# 6. 准入控制

# 6.1. 关于准入控制

- 天珣具备业界最完善的计算机终端准入控制机制,从应用层和 边界层到客户端,提供了客户端准入和应用准入等多种准入控 制手段,确保只有通过身份验证和安全状态检查的计算机终端 才能接入内网并进行受控访问,对非法的或存在安全隐患的计 算机终端进行隔离和修复,构建出完善的"内网安检系统", 从源头上有效减少内网安全漏洞。
- 天珣支持基于策略网关的应用准入控制及基于计算机终端安全状态的客户端准入控制,更可与启明星辰天清汉马 USG 一体化安全网关进行联动,确保只有通过身份验证和安全状态检查的计算机终端才能接入内网,变被动防御为主动防御,为内网的安全合规提供强制性保障。天珣的多种准入控制手段可灵活组合,有效保护用户投资。
- 天珣的多层准入控制机制,彻底颠覆了传统内网安全管理被动
   管理的局面,为终端安全合规提供了强制性的保障能力。





天珣多层准入控制逻辑图

# 6.2. 网络准入

\*该章节功能仅适用于高级版和增强身份认证高级版

# 6.2.1. 关于网络准入

- 网络准入认证支持各种认证策略,包括:支持有线网络准入 (标准 802.1x、Eou)和无线网络准入(标准 802.1x),基于 仅验证客户端运行,用户认证,用户、IP、MAC 组合认证, 可信 MAC 认,可信 GUID 认证和接入设备端口绑定。
- "标准的 802.1x"和 "EoU 认证"认证过程中支持组合认证,不支持组合绑定。

注意:这并不说明标准的 802.1x 不支持 User-IP, MAC-IP 组合 自动进行绑定,若网络准入中不配置认证策略,但配置了基于终端的 User-IP 或 MAC-IP 组合,当网络准入认证成功,客户端到 策略服务器取策略时,可自动改回指定的 IP 地址。

### 名词解释

"RADIUS Server":网络准入认证的基本选项,包括选用网络准入认证策略、RADIUS 认证服务器 IP 地址和启用网络准入控制的交换机或路由器等。交换机的配置在"基本配置"的"网络设备配置"里面配置。



- "可信 MAC 认证实时授权":如果在认证策略中启用了扩展可信 MAC 认证,那么系统在网络准入认证过程中将会拒绝可信任 MAC 列表之外的客户端,管理员可在此对非可信MAC 地址的客户端进行授权。
- "可信 GUID 认证实时授权":如果在认证策略中启用了扩展可信 GUID 认证,那么系统在网络准入认证过程中将会拒绝可信任 GUID 列表之外的客户端,管理员可在此对非可信GUID 的客户端进行授权。
- "免认证 MAC 地址列表":如果在认证策略中启用了该策略,在免认证 MAC 地址列表里面添加了相应的 MAC 地址,则对在该列表中的 MAC 地址所对应的设备不进行网络准入认证,前提是该设备没有安装客户端,如果该设备安装了客户端,那么接入网络时,还是会对它进行准入认证。
- "VLAN 信息":本系统支持基于用户和 MAC 的动态 VLAN 功能,在此可查看 VLAN 与用户或 MAC 的关联信息。 但此处不能用于设置动态 VLAN。

下图是网络准入控制范围示意图。



## 6.2.2. RADIUS Server 页面

### 配置介绍



RADIUS Server	可信MAC认证实时授权可信GUID认	、证实时授权 免认证MAC地址列表
RADIUS Server		
RADIUS Server名称	初始radius服务器	*
描述		A
		*
IP地址	10.201.1.204	*
认证策略		
网络准入类型	◎ 标准802.1x	
	© E₀U	
基本认证	◎ 仅验证客户端运行	
	◉ 用户认证	
	◎ 可匿名的用户认证	
选择启用的日求服务	☑ 本地用户	
用户、IP、MAC组合认证	◎云白田	
	◯ 小油用	
可信MAC认证	◎ 不启用	
可信GUID认证 (eou认证无效)	◎ 不启用	
MAC免认证 (无线网络认证无效)	◎ 不启用	
日本林本市、印名地址		

給证客戶編是否满足安全状态 (王總同時以近子像)	华 不输送	
Construction of the Construction	○安全状态完整时旅行,不完整时给出提长后放行	
	○安全状态完整时做行,不完整时始出揭示后切换到无效mac堵址时推定的NLAM	
	○ 安全状态完整时做行,不完整时始出提示原不做行	
息用唯人控制的交换机成路由器	查查万無相 +对我人这些汉美式和防由期的共调实施准人反制	
创建状态	主局	
创建有	admini a trator	

Bestonswede	1	P TROLE HROMAN
王theic通过HARD	P	P THERE HERE
ROMAN AND A		
Similan Brain		
(Listland)		
CLientlem@#200.	-	
Chertenillich	permit udp may may eq 21002 permit udp may eq bootpo may eq heatpz permit udp may may eq domain dens iong are may	- auguranes [1]
BAD BID MID KS	permit ip any any	-
无的ex:他说时说(x)。	persit odp may may sg 21382 persit odp may sg hostpe may sg hostpe persit odp may may sg domain	
	ELICITATION AND A MERITAL LOGAL	THE PERSON IN THE PARTY OF



配置项:	兑明
RADIUS Server 名称	用以标记该 RADIUS 服务器,建议名称能够明确 代表该 RADIUS 的真实服务器。
描述	用以对该服务器的角色等详细描述,方便日常管 理。
IP地址	Radius 服务器的 IP 地址
认证策略	
网络准入类型	选择网络准入认证的协议类型。天珣网络准入目前 支持"标准 802.1x", "EoU"(即 Cisco EAP over UDP 类型)。 默认使用标准 802.1x 即可满足大部分用户需求。
基本认证	为方便管理,可以选择"仅验证客户端运行",该 选项只需安装天珣客户端,终端身份即可认证通 过。 "用户认证"用户身份的确认方式,如果该用户没 有帐号和密码,则被交换机强制网络阻断。 "可匿名的用户认证"特指在基于用户认证的情况 下,允许无用户帐号的终端匿名登录网络。可匿名 的用户认证仅在用户认证方式下有效,无用户认证 配置就无法使用该模式。
选择启用的目录服务	只有选择了"用户认证"或者"可匿名的用户认证"时,才能应用此选项,默认只有"本地用户",也可以自己建立其他本地用户认证或 AD 域用户认证,其配置在"基本配置"的"本地用户"和"用户组"里面配置。
用户、IP、MAC 组合认	在网络准入的认证过程中直接对该终端的组合信



证	息确认,若组合条件不满足要求,直接网络阻断并				
	提示。仅在漫游 IP 网段 802.1x 的情况下,可以基				
	于用户绑定信息自动更改终端的 IP 地址。				
	此选项与"可信 MAC 认证实时授权"结合使用。				
	选中可信 MAC 认证,若某终端的 MAC 地址不在				
	可信 MAC 列表中,将被网络阻断并提示修复。管				
可信 MAC 认证	理员确认该 MAC 可信后可以在线实时授权。若该				
	MAC 地址是来访人员,根据其来访的时间,可以				
	分配准入的时间段,如果超过该时间段则网络阻				
	断。				
	此选项与"可信 GUID 认证实时授权"结合使用。				
	选中可信 GUID 认证,若某终端的 GUID 地址不在				
	可信 GUID 列表中,将被网络阻断并提示修复。管				
可信 GUID 认证	理员确认该 GUID 可信后可以在线实时授权。若该				
	GUID 是来访人员,根据其来访的时间,可以分配				
	准入的时间段,如果超过该时间段则网络阻断。				
	可选择客户端在认证时是否检查其中心服务器 IP				
是否检查中心服务器地	地址是否与 radius 服务器接收策略的中心服务器地				
址	址一致,如不一致则认证失败。				
	主要有四种验证方式:(1) <b>不验证</b> ;即不对客户端				
	的安全状态做任何验证,就算客户端的安全状态不				
	满足,也不会弹出任何提示;(2)安全状态完整时				
队过安白洲目天进口安	<b>放行,不完整时给出提示后放行</b> ;当客户端的安全				
<u>验证各户</u>	状态不完整时, 会弹出提示框, 但是网络依然是通				
主认心	的;(3) 安全状态完整时放行,不完整时给出提示				
	后切换到无效 MAC 地址时指定的 VLAN;注意这				
	里要在配置交换机时,让交换机支持动态 VLAN,				
ŧ	并且在下面的"无效 MAC 地址 VLANID"里面配				



	置 VLANID; (4) 安全状态完整时放行,不完整时			
	<b>给出提示后不放行</b> ;当客户端安全状态不完整时,			
	会弹出提示框,并且阻断网络。			
启用准入控制的网络设	认证策略中最重要的选项,即勾选 RADIUS 接受			
备	认证的网络设备。			
	即该页面创建的权限,如果是全局管理员创建则状			
创建状态	态为全局,所有管理员均可以看到该配置,如果是			
	本地管理员,则其他本地管理员无法看到该页面。			
创建者	标记了该策略是由哪个管理员创建。			
802.1x 选项	·			
	若某终端、用户未被配置 VLAN 信息,则交换机			
默认 VLANID	会将之切换至默认 VLAN 中,如果不指定 VLAN,			
	则使用交换机默认设置。			
	在可信 MAC 认证的前提下,如果某终端未被授权			
无效 MAC 地址 VLANID	为可信 MAC,则将之切换至该 VLAN,如果指定该			
	VLAN,则拒绝访问(需要管理员授权接入网络)			
EOU 选项				
	用于在路由器上启用 EoU 认证,交换机认证可以			
Clientless 用尸名	忽略此选项,默认值为 Clientless			
	用于在路由器上启用 EoU 认证,交换机认证可以			
Clientless 密码	忽略此选项,默认值为 Clientless			
	当某终端确认未安装天珣客户端时,任何 http 访问			
	将被准入交换设备重定向至该 URL。该 URL 可以			
Clientless 提示 URL	是任何 URL, 但要确保 Clientless 的 ACL 对此有做			
	明确例外排除,例如:如果重定向的 URL 为			
	http://192.168.0.1/index,			



	那么Clientless的ACL中需要添加一条ACE: permit
	tcp any host 192.168.0.1 eq www。默认值为:
	http://192.168.0.236:8833/download.(若天珣策略服
	务器的 IP 地址为 192.168.0.236)
	即如果终端未安装天珣客户端时,交换准入设备将
	分配的 ACL,如下均为必须 ACE。
	permit tcp any host 192.168.0.236 eq 8833(若天珣策
	略服务器的 IP 地址为 192.168.0.236,该 ACE 允许
	所有客户端访问客户端下载页面)
Clientless 的 ACL	permit udp any any eq 21862
	permit udp any eq bootpc any eq bootps
	permit udp any any eq domain
	deny icmp any any
	deny ip any any
	如果终端安装有天珣客户端,并且开启了 EoU 认
	证选项,网络准入设备将分别下面的 ACL,即允
验证通过时的 ACL	许访问任何网络。
	permit ip any any
	如果 EoU 中有配置可信 MAC 认证, 而该终端 MAC
	地址不在可信 MAC 域中,则走此 ACL。注意:走
	此 ACL 的终端必须是已经安装有天珣客户端的
	PC。默认值同 Clientless 的 ACL。
无效 MAC 地址时的	permit tcp any host 192.168.0.236 eq 8833
ACL	permit udp any any eq 21862
	permit udp any eq bootpc any eq bootps
	permit udp any any eq domain
	deny icmp any any
	deny ip any any
	1



**注意**:如果网络中有多台 RADIUS 服务器,不同的服务器可仅为 指定的那些交换机提供服务,以确定该 RADIUS 服务器的最大负 载。但需避免出现某交换机**仅在主 RADIUS 服务器上有可信任关 系**,否则当主 RADIUS 服务器宕机时,该交换机将强制阻断所有 接入终端!

当启用"网络准入"的认证策略时,则"基本配置"里面的"IP 组"的用户认证策略则尽可能不要启用,避免发生冲突。

**建议:** 网络中至少部署两台 RADIUS 服务器,而两台 RADIUS 服务器关联的交换机完全相同。

注意:标准的 802.1x 准入下,天珣支持动态 VLAN 功能。如果某用户、终端未分配其 VLAN 号,可以将之切换至默认 VLAN,如果 某终端 MAC 地址不在可信 MAC 表中,也可以以将之切换至指定的 VLAN。

注意: clientless 提示 URL 页面建议配置成 http://中心服务器 IP:8833/download 直接给用户一个下载提示页面,并在 clientless 的 ACL 中放开对中心服务器 IP 的 8833 端口限制,假设配置成一个 80 端口的访问页面,那么客户端在弹出页面时将需要花费很长时 间。

### 启用准入控制的网络设备页面

点击"查看及编辑"配置链接可勾选 Radius 接受认证的交换机 和路由器:





当配置的交换机或者路由器数量较多时,还可以根据相关的属性 对他们进行查找。交换机和路由器的相关配置在"基本配置"的 "网络设备配置"里面配置。

# 6.2.3. 可信 MAC 认证实时授权页面

### 配置介绍

当客户机安装天珣客户端并接入交换机端口(或通过无线连接)时, 本系统会自动获取其 MAC 地址并与可信 MAC 列表对比,以确认 其是否属于内部终端,若不是则拒绝其接入网络,并将其列入未授 权接入列表中。

RADIUS Server	HEMACHIERH	n atto	ID认证实时授权	免认证MAC	地址列表	VLAN信息
可信MAC认证	实时授权					
选择董商起始时间	11/2/2012 5:10 PM	2 全部職	S BERADIN	服务苦蜜庵	製油	
		注: BC地	umilient eikst	Eifenders服务器管	调"进行更新。	
初始radiaの販売	8					
三初始vadius服务	書刷董					
and the later of t	用料	交換机印建始	交換机端口	STRUMPLES	或功要入	帮权
001F3C013685	11/3/2012 5:10:54 38	10.201.1.110		无	拒绝	<b>BIO</b>

点击"授权",管理员可以对其进行设置。





配置项:	说明
可信 MAC 策略	右边有个下来选项,可以选择对应的策略。
MAC 地址	被拒绝的非可信 MAC 地址。
主机名	填写主机名,便于查询管理。
MAC 地址有效期限制	开启 MAC 地址有效期限制, MAC 地址只能在指定的时间范围内通过认证,超出时间范围将再次被拒绝。
MAC 地址有效期起始时间	MAC 地址有效期起始时间。
MAC 地址有效期结束时 间	MAC 地址有效期结束时间。
802.1X 选项 VLANID	为MAC地址分配VLAN,客户端通过认 证后,所接的交换机端口将被自动划分至 指定的VLAN,默认值为0,则表示默认 交换机的配置。



授权	
----	--

给被拒绝的终端授权其进入网络。

设置完成,点击保存,进入即时更新规则一>更新 Radius 规则,即时更新 Radius 服务器的规则,即可使设置生效。

**注意:**如果某终端授权时间结束,但其并未关机或与网络断开连接, 而且交换机并未出发重认证,该终端仍旧未被阻断,直到 802.1x 触发重认证。

### 6.2.4. 可信 GUID 认证实时授权页面

### 配置介绍

当客户机安装天珣客户端并接入交换机端口时,本系统会自动获取 其 GUID 地址并与可信 GUID 列表对比,以确认其是否属于内部终 端,若不是则拒绝其接入网络,并将其列入未授权接入列表中。

RADRUS Server	可當MAC這這天相變收	1 11	GUIDARENN	RIL RUEMA	C地址列表	VEANE	2 ) -			
₩ GCUIDIL #	实时授权									
GREADER	11/2/2012 5112 20	3	is talis at al	AARTHEEMER	SLE2					
		(±)	ADADIA ZEL C. M	A BERNORSESS	E.EU68+					
-										
Elliptenen luka	E Contraction (									_
-初始radine服务]	理解算									
4418		15.65	60 M.U.	1100	184	rttal 3	110-11	STREET.AR	成功的人。	
Announcement and the	INT. AND POSTAL AND	A. Sec.	NOTESTIC DEPC.	112500000 0.00 at 1	10.000	100			1140	100 M



9 可信GUID線人設設 - Bicrose	oft Internet Explo	rer		
RADIUS Server名称172. 可信ourD策略	. 25. 0. 226		*	-
OUID				
MAC±BLtE	001e9096a07a			
主机名				
GUID社证有效期限制 GUID社证有效期起始时间	中省の是			
GUID认证有效期结束时间				
802.1X选项VLANID	0			
ROVIA: 79 ACL				
注:着 <b>想有*号的项目必须输入。</b>	保存 取消			
4				- L L Č



配置项:	说明
可信 GUID 策略	选择此 GUID 所属的 GUID 策略
GUID	被拒绝的非可信 GUID
MAC 地址	被拒绝的非可信 MAC 地址。
主机名	填写主机名,便于查询管理。
GUID 地址有效期限制	开启 GUID 地址有效期限制,GUID 地址 只能在指定的时间范围内通过认证,超出 时间范围将再次被拒绝。
GUID 地址有效期起始时	GUID 地址有效期起始时间。
GUID 地址有效期结束时 间	GUID 地址有效期结束时间。
802.1X 选项 VLANID	为 GUID 分配 VLAN,客户端通过认证后, 所接的交换机端口将被自动划分至指定的 VLAN,默认值为 0,则表示默认交换机的 配置。
授权	给被拒绝的终端授权其进入网络。

设置完成,点击保存,进入即时更新规则一>更新 Radius 规则,即时更新 Radius 服务器的规则,即可使设置生效。

**注意:**如果某终端授权时间结束,但其并未关机或与网络断开连接, 而且交换机并未出发重认证,该终端仍旧未被阻断,直到 802.1x 触发重认证。



# 6.2.5. 免认证 MAC 地址列表页面

### 配置介绍

天珣策略系统支持 MAC 免认证功能,在此处添加免认证 MAC 地址列 表,则对在该列表中的 MAC 地址所对应的设备不进行网络准入认 证,前提是该设备没有安装客户端,如果该设备安装了客户端,那 么接入网络时,还是会对它进行准入认证。 点击"**添加**",则可配置策略,策略名称可自定义:

RADIUS Server	可信MAC认证实时授权	可值GUID认证实时授权	免认证MAC地址列表	VLAN信息
免认证mactitut	管理 添加			
<b>毎以近期に伸展到本</b>				
345 BC BE 4880 315 3E 73 4E			帮助	
新聞名称	814	062 A	設置	
		14648		

在生成的策略中进行"设置",点击"添加",即可填写免认证的

MAC 地址。

添加免认证TAC地址	添加 返回			
MAC+也+上			查询	重置
■AC地址		主机名		
AABBCCDDEEFF		win		
1				

注: 启用免认证 MAC 功能时,还需要在交换机上面配置相关的命令,具体情况请

参考"网络准入其他组件配置"。

## 6.2.6. VLAN 信息页面

### 配置介绍

天珣策略系统支持基于用户和 MAC 的动态 VLAN 功能, 如果在可



信 MAC 或用户, IP, MAC 组合中配置了 802.1X VLAN 信息,

可以在 VLAN 信息页面查看到该 VLAN 。

RADIUS Serv	er 可信MAC认证	实时授权 可信GUII	D认证实时授权	<b>免认证MAC地址列表</b>	VLANCE
VLAN信息				-	
VLATIO	天联的南户	天氣的加仁	关联的问题		
1	1	1	1		

点击关联用户或关联 MAC 可查看与 vlan 相关联的用户或 MAC 信

息,同时也可删除相关联的用户和 MAC。

### 6.2.7. 网络准入配置要点

- 1、点击 RADIUS Server "添加" 按钮,添加 Radius 服务器;
- 2、输入 "RADIUS Server 名称"、"IP 地址";
- 3、配置在网络准入过程中的认证策略;
- 4、点击启用准入控制的交换机或路由器"查看及编辑"链接页面;
- 5、在链接页面里面勾选上对应的交换机或者路由器;
- 6、勾选完对应的设备之后,点击"确定"跳转到 RADIUS Server 配置页面,再点击"保存";
- 7、点击"即时更新策略->更新 RADIUS 策略",点击"更新 RADIUS 服务器策略"。

将安装有天珣客户端的终端接入启用 802.1x 认证的交换机,即可访问网络。

注意: RADIUS 服务器必须手工更新策略,否则无法获取新的认证 策略;更新规则前需确认 RADIUS 服务器 IP 地址存在于 IP 组中。

### 6.2.8. 网络准入其他组件配置

天珣内网安全风险管理与审计系统网络准入控制认证方式包括 802.1x 验证和 Cisco EOU 验证两种。由 3 部分组成:天珣内网安



全风险管理与审计系统 ESCC 客户端, ESRadius 服务器, 提供 802.1x 功能或者 EOU 功能的交换机/路由器。其中 ESCC 客户端和 ESRadius 服务器由启明星辰开发提供。交换机由交换机厂商提供,不同厂商 的 802.1X 配置方法存在较大区别,对交换机的配置,下面只介绍 配置原理要点,然后以Cisco 2950(12.22(EA1))、Cisco 3550 和华 为交换机为例说明配置过程。

### 客户端配置

打包客户端:在服务器使用客户端打包工具生成客户端安装包。打 包时必须选择使用 802.1x 交换机认证才能实现 802.1X 认证功能。 客户端安装完成重启后,802.1X 模块即可生效。

3 客户端打包工具		X				
輸入中心服务器PP地址 指定安装目录	10 . 201 . 1 . 204					
安装模式	(• 音通 () 目动 () 静默					
	<ul> <li>☑ 使用802.1%交換机认证</li> <li>☑ 被用EOU认证</li> <li>□ 网络中有迈普S3150交换机,否则不建设勾选</li> <li>□ 隐藏客户端图标</li> <li>□ 支持单点图陆</li> <li>☑ 文件审计模块</li> <li>☑ 移动存储管理模块</li> <li>☑ 软件分发模块</li> </ul>					
生成客户端安装包						
转到客户端安装包的存祉目录						
将客户编安装包复制到中心服务器的下载目录						

如需要启用EOU功能,打包时选择EoU。或者通过需要修改ESCC. ini

文件: [LOG] LogFile = log ESCC. logBakLogFile = log\ESCC.log\_bak MaxLogLine = 100000Backup = 1Level = 2; 1 - DEBUG 2- INFO 3- WARN 4- ERROR 5- FATAL



[Firewall]

PerPacketCheck = 0

[ESCC]

RequestMethodV2 = 1

### EnableEOU = 1

将最后一行的 EnableE0U=1 即可。

#### Radius 服务端配置

Raidus 服务端位于策略系统中心服务器或本地服务器上。要求的操作系统为Windows2000/2003 Server版。

如果该计算机已经安装过 IAS 服务,请先卸载该服务,或者停止该服务并设置为已禁用。

运行安装光盘,点击安装 Radius 服务组件,启动安装程序。

安装完成后,请进入 ESRadius 服务器的安装目录,一般默认为 C:\Program Files \ESRadius,打开 ESRadius.ini 文件,文件内 容如下所示:

[Radius]

IPAddress = 0.0.0.0

; If a multi-ip host, you need set the listening ipaddress of radius server

; when IPAddress=0.0.0.0, radius server is listening on all ipaddress

### EAPMD5Channel = 1

; Some switchs, liking ZTE and Huawei's Product, only support EAP\_TYPE\_MD5(4), which can't transport other type EAPOL Packages

; Set EAPMD5Channel = 1, Enable set EAP Data Type as MD5's type



[LOG] LogFile = log\ESRadius.log BakLogFile = log\ESRadius.log bak MaxLogLine = 100000Backup = 1Level = 1: 1 - DEBUG 2- INFO 3- WARN 4- ERROR 5- FATAL 这些选项一般可按照默认设置,按需修改。 IPAddress = 0.0.0.0, 当安装 ESRadius 组件的计算机有多网卡时, 需要在此指定 radius server 监听的 IP 地址。 EAPMD5Channel = 1, 如果交换机只支持 EAP\_TYPE\_MD5(4), 例如 中兴、华为交换机,那么此选项设置为1,如果交换机还支持其他 类型的 EAPOL Packages, 例如 Cisco 交换机,那么此选项可设置 为0。 文件修改保存后, 请重新启动 ESRadius 服务, 使配置生效。 天珣内网安全风险管理与审计系统 Radius 服务器组件安装后, 会 在 iis 默认 web 站点中,新建一个名为 ESRadiusWS 的虚拟目录, 这个虚拟目录的运行需要 Dot Net Framework 2.0 的支持。 认证日志 查询客户端接入交换机时,进行 Radius 认证的日志。 管理员可查询指定 Radius 服务器的认证日志。

当日志数据库比较大时,可选择删除指定时间之前的日志,或者一 键优化日志数据库。

### 交换机配置

为使用天珣内网安全风险管理与审计系统的 802.1X 验证功能,需要交换机提供以下功能支持:

1 支持 802.1X 功能

2 支持 802.1X 的 EAP over Radius 认证功能



3 支持 Radius 协议

为使用天珣内网安全风险管理与审计系统的 EOU 验证功能, 需要交

换机/路由器提供以下功能支持:

- 1 支持 EOU 功能
- 2 支持 EAP over UDP 认证功能
- 3 支持 Radius 协议

### Cisco2950 的配置

### (12.1(14)EA1 以上版本)

以下材料来自于 Cisco 文档: Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide (full book i.pdf

配置前,做以下设定:设置 Cisco 交换机 IP 地址为 192.168.0.2, 设置 ESRadius 服务器 IP 地址 192.168.0.236,交换机和 ESRadius 服务器通讯的 Radius 密钥为 123456

以下部分是已经完成的配置,我们在交换机的端口7启用了802.1x

认证。接下来看一下配置步骤。

Switch#show running-config Building configuration... Current configuration : 1519 bytes ! version 12.1 no service pad service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname Switch

۱



aaa new-model aaa authentication dot1x default group radius enable secret 5 \$1\$GyoJ\$VX3N1qYOnVH3hXjmVPYB5/ enable password 654321 ! ip subnet-zero ! ! spanning-tree mode pvst no spanning-tree optimize bpdu transmission spanning-tree extend system-id dot1x system-auth-control ! ! ! ! interface FastEthernet0/1 ! interface FastEthernet0/2 ! interface FastEthernet0/3 ! interface FastEthernet0/4 ! interface FastEthernet0/5 ! interface FastEthernet0/6 ! interface FastEthernet0/7



switchport mode access dot1x port-control auto dot1x timeout reauth-period dot1x reauthentication spanning-tree portfast ! interface FastEthernet0/8 ! interface FastEthernet0/9 1 interface FastEthernet0/10 ! interface FastEthernet0/11 ! interface FastEthernet0/12 1 interface FastEthernet0/13 ! interface FastEthernet0/14 ! interface FastEthernet0/15 ! interface FastEthernet0/16 ! interface FastEthernet0/17 ! interface FastEthernet0/18 ! interface FastEthernet0/19



! interface FastEthernet0/20 ! interface FastEthernet0/21 ! interface FastEthernet0/22 ! interface FastEthernet0/23 ! interface FastEthernet0/24 ! interface Vlan1 ip address 192.168.0.2 255.255.255.0 no ip route-cache ! ip http server radius-server host 192. 168. 0. 236 auth-port 1812 acct-port 1813 key 123456 radius-server retransmit 3 1 line con 0line vty 0 4 password 123456 line vty 5 15 password 123456 ! ! end

### 1. 进入配置命令模式



# config terminal

#### 2. 配置 Radius 认证服务器

启用认证

# aaa new-model

设置 802.1X 使用 radius server 组中的所有 radius server 进行

认证

# aaa authentication dot1x default group radius

 $\ensuremath{\texttt{\#}}$  aaa authorization network default group radius

添加 ias 到 radius server,其中 host 后面的 IP 地址为 IAS 服务

器地址, auth-port 和 acct-port 为标准的 Radius 端口, key 为交

换机和 Raidus 服务器通讯密钥

# radius-server host 192.168.0.236 auth-port 1812 acct-port 1813 key 123456

#### 3. 启用 802.1X

# dot1x system-auth-control

 配置7号端口使用802.1X认证,若交换机支持Guest VLAN, 那么当认证不通过时,则将其分配至Guest VLAN

# interface FastEthernet0/7

- # switchport mode access
- # dot1x port-control auto

# dot1x guest-vlan 10 (for example : guest-vlan id =10)

# dot1x host-mode multi-host ( 启 用 交 换 机 端 口 的

multiple-hosts 模式,以使交换机可下接 hub 进行认证)

# end

#### 5. 配置7号端口的重认证周期

可选项,配置 802.1X 重认证的周期,以秒为单位,默认为 3600 秒(1 小时),当重认证时,如果网络端口接入其他没有运行天珣 内网安全风险管理与审计系统的计算机,端口会立刻封闭。

- # interface FastEthernet0/7
- # dot1x reauthentication



# dot1x timeout reauth-period 3600

# end

6. 保存当前配置作为启动配置

# copy running-config startup-config

#### 7. 如何禁用 dot1x

禁用 AAA: #no aaa new-model

禁用 802.1x 的 AAA 认证: #no aaa authentication dot1x default

group radius

禁用 802.1x 认证 AAA: #no aaa authorization

禁用端口的 802.1x: no dot1x system-auth-control

#### 8. 批量端口配置

对 2-24 端口进行批量配置

#interface range FastEthernet0/2 - 24

#switchport mode access
#dot1x port-control auto
#dot1x host-mode multi-host
#dot1x timeout reauth-period 900
#dot1x reauthentication
#spanning-tree portfast
#end

注意: CISCO 的交换机如果是远程使用 telnet 登录到交换机进行 配置的话,请千万记得配置 aaa authentication login default line 命令(不同型号交换机可能命令略有不同)。此命令作用是将 telnet 时进行的认证放在交换机本地,如果不配置的话,假如以 前 telnet 交换机只需要输入密码的话,那么在下次进行 telnet 登录时,交换机将会提示要求输入用户名和密码进行认证。

注意:如果有多台 radius 服务器进行备份,要保证主 radius 服务



器出问题时可以正常切换,需要另外配置 radius-server deadtime 1 命令,其中1表示 radius 服务器认证超时时间。

### Cisco EAPoUDP NAD 配置 配置 Radius 服务器

aaa new-model

aaa authentication eou default group radius aaa session-id common radius-server host 192.168.0.223 auth-port 1812 acct-port 1813 key 123456 radius-server vsa send authentication 路由器中配置 Radius 通讯端口 ip radius source-interface FastEthernet0/0

### 路由器的 EOU 认证

#### 配置 EOU 认证模式

ip admission name TEST eapoudp

可以配置只在某些情况下启用 EOU, 通过设置 ACL 实现

ip admission name AVERT eapoudp list 102

access-list 102 deny udp any host 10.10.30.10 eq domain

access-list 102 deny tcp any host 10.10.20.10 eq www

access-list 102 permit ip any any

#### 对某些主机的排除设置

identity profile eapoudp

device none-authorize ip-address 192.168.0.223 policy NACless

device none-authorize ip-address 192.168.0.1 policy NACless

identity policy NACless

access-group clientException


ip access-list extended clientException

permit ip any any

### Clientless 认证设置

eou clientless username clientless

eou clientless password password

eou allow clientless

## 配置 EOU 通讯端口

interface FastEthernet0/0

ip address 192.168.0.200 255.255.255.0

ip access-group 101 in

ip admission TEST

access-list 101 permit udp any host 192.168.0.200 eq 21862

## URL-Redirect HTTP Server 配置

ip http server

no ip http secure-server

#### 允许 EOU 日志

eou logging

## 交换机的 EOU 认证配置

交换机上的 EOU 认证 (L2 IP Validation) 通过 EOU 认证协议完成。但 EOU 的认证激活模式与 802.1X 类似。当交换机检测到启用了 L2 IP Validation 的端口上有新的 IP 地址加入时,就会发起 EOU 认证。

只有配置为 switchport mode access 的端口才能启用 EOU。

## L2 IP Validation 的启用

1 创建 NAC 规则

ip admission name nac eapoudp

2 定义 NAC 使用的 accesslist

在认证端口在没有认证的情况下会使用这里定义的 accesslist。



可定义两种 accesslist: Port Access List 和 IP Access List。 如定义 Port Access List, 语法如下: access-list 5 permit any any 如定义 IP Access List,则如下: ip access-list extended NAC // 允许 EOU 通信 permit udp any any eq 21862 permit udp any eq bootpc any eq bootps // 允许 DHCP permit udp any any eq domain // 允许域名解析 // 拒绝 ICMP deny icmp any any // 拒绝其他 IP 通信 deny ip any any 3 对需要进行认证的端口启用 NAC 规则 a, Port Access List interface fa0/1ip access-group 5 in ip admission nac b, IP Access List interface fa0/1ip access-group NAC in ip admission nac 4 配置 IP Device Tracking ip device tracking probe count 2 ip device tracking probe interval 60 ip device tracking 对某些主机的排除设置 identity profile eapoudp device none-authorize ip-address 192.168.0.223 policy NACless none-authorize ip-address 192.168.0.1 policy device NACless 136



identity policy NACless
access-group clientException
ip access-list extended clientException
permit ip any any

## EOU 的参数配置

具体指令参考 Cisco 的 NAC 配置指南。需要配置的指令如下 eou default eou logging eou timeout status-query 1800 eou timeout revalidation 900 eou revalidate

由于天珣内网安全风险管理与审计系统不支持状态查询,需要保证 重认证超时<状态查询超时(5s<sup>~</sup>30min),上面将重认证超时设置为 15min,状态查询超时设置为 30min

### Clientless 的认证设置

交换机和路由器不同,不支持使用 Clientless 用户名密码向 Radius 认证 Clientless 用户,而是通过 Radius 请求的属性辨别 是 Clientless 认证还是正常的用户认证。

配置指令

eou allow clientless

## URL 重定向 ACL 的设置

当指定交换机对客户端进行 URL 重定向时,需要事先在交换机上设置用于重定向的 ACL, ACL 名称固定为 url-redirect-acl。当请求与重定向 ACL 匹配时,客户端的 HTTP 请求会被重定向。

下面的 ACL 定义将到 http://192.168.0.223 的访问进行重定向。

ip http server

ip access-list extended url-redirect-acl

permit tcp any host 192.168.0.223 eq www

建议将此 URL 设置为中心服务器的客户端下载页面,即提示



http://服务器 IP:8833/download

**注意**:不同的交换机有可能设置 radius 组时的命令不尽相同,不可死搬硬套。例如有时需要定义一个 radius 组让交换机去调用,并在这个组里配置 radius 服务器, aaa group server radius XXX, 然后用 aaa authentication eou default group XXX 进行调用。

#### 华为交换机的配置

不同型号的交换机配置步骤可能有所不同,本配置用例仅供参考。 配置前,做以下设定:设置 huawei 交换机 IP 地址为 192.168.0.5, 设置 ESRadius 服务器 IP 地址 192.168.0.236,交换机和 ESRadius 服务器通讯的 Radius 密钥为 123456

我们将在交换机的端口 8 启用 802.1x 认证。接下来看一下配置步骤。

# 设置接入控制方式,该命令可以不配置,因为端口的接入控制在 缺省情况下就是基于 MAC 地址的

[Quidway] dot1x port-method macbased interface ethernet 0/8

# 设置 802.1x 用户的认证方法,目前提供 3 种认证方法: PAP 认证、CHAP 认证、EAP 中继认证。缺省情况下,华为交换机 802.1x
用户认证方法为 CHAP 认证。此处需要修改设置为 EAP 认证。
[Quidway] dot1x authentication-method eap

# 创建 RADIUS 组 dot1x 并进入其视图 [Quidway] radius scheme dot1x

# 设置主认证/计费 RADIUS 服务器的 IP 地址 [Quidway-radius-dot1x] primary authentication 192.168.0.236



# 设置主认证/计费 RADIUS 服务器的 IP 地址

[Quidway-radius-dot1x] primary accounting 192.168.0.236

# 设置系统与认证 RADIUS 服务器交互报文时的加密密码
 [Quidway -radius-dot1x] key authentication 123456
 [Quidway -radius-dot1x] key accounting 123456

# 指示系统从用户名中去除用户域名后再将之传给 RADIUS 服务器
 [Quidway-radius-dot1x] user-name-format without-domain
 [Quidway-radius-dot1x] quit

# 创建用户域 dot1x,并进入其视图 [Quidway] domain dot1x

# 指定"dot1x"为该用户域的 Radius 方案 [Quidway-isp-dot1x] radius-scheme dot1x [Quidway-isp-dot1x]quit

# 指定交换机缺省的用户域为"dot1x" [Quidway] domain default enable dot1x

# 开启 E0/8 的 802.1x 认证 [Quidway] dot1x interface Ethernet 0/8

# 开启全局 802.1x 特性 [Quidway] dot1x

# 保存设置



[Quidway] quit <Quidway> save

新版 IOS 的 H3C 交换机配置里已经不支持 scheme radius-scheme 命

令,这条命令被三条命令所取代,这三条命令是: authentication default radius-scheme dot1x authorization default radius-scheme dot1x accounting default radius-scheme dot1x

注意: 华为交换机也存在和思科交换机同样的 telnet 密码认证问

题,解决的方法与思科交换机原理相同,将 telnet 密码认证放在 本地进行。 User-interface vty 0 4 Authentication-mode password Set authen password cipher XXXXXX

## 锐捷交换机的配置

不同型号的交换机配置步骤可能有所不同,本配置用例仅供参考。 配置前,做以下设定:设置锐捷交换机 IP 地址为 192.168.0.249, 设置 ESRadius 服务器 IP 地址 192.168.0.191,交换机和 ESRadius 服务器通讯的 Radius 密钥为 123456 我们将在交换机的端口 1 启用 802.1x 认证。

#### 验证通过的交换机软硬件版本:

System hardware version : 3.2 System software version : 1.69 Build Aug 2 2007 Release System BOOT version : RG-S2126G-BOOT 03-03-02 System CTRL version : RG-S2126G-CTRL 03-11-02 Running Switching Image : Layer2

## 完整的参考配置如下:



start#sh run System software version : 1.69 Build Aug 2 2007 Release Building configuration... Current configuration : 731 bytes ! version 1.01 no enable services web-server hostname start vlan 1 ! vlan 11 ! radius-server host 192.168.0.191 aaa authentication dot1x enable secret level 1 5 !, tZ[V/, U+S(\W&-G1X)sv'~H.Y\*T7+. enable secret level 15 5 \$2kE, 1u 3h1&-8U04in'.tj9Qjo+/7R: ! interface fastEthernet 0/1dot1x port-control auto dot1x dynamic-vlan enable ! interface vlan 1 no shutdown ip address 192.168.0.249 255.255.255.0 !



no dotlx filter-nonRG-su enable dotlx auto-req no dotlx auto-req user-detect dotlx auto-req req-interval 180 dotlx re-authentication radius-server key 123456 snmp-server community public ro line vty login local ! **End** 

## 配置步骤:

1、配置 radius 服务器地址,项目部署时请加备用 radius-server。 radius-server host 192.168.0.191

2、全局启用 dot1x aaa authentication dot1x

3、进入接口启用 dot1x interface fastEthernet 0/1 dot1x port-control auto

4、关闭非锐捷客户端的过滤 no dot1x filter-nonRG-su enable

5、当交换机下接 HUB 时,需打开交换机主动请求认证的功能,并 设置发送间隔。

锐捷交换机是以主动发送认证包的方式支持基于 MAC 地址的验



证的。 dot1x auto-req no dot1x auto-req user-detect dot1x auto-req req-interval 180

6、打开重认证功能

dot1x re-authentication

7、设置与 radius server 通讯的密钥 radius-server key 123456

## 免认证 MAC 的相关配置

1、思科交换机配置要点:

在正常配置完 802.1X 准入之后,在端口下输入"mab eap" 或 "dot1x mac-auth-bypass eap" 命 令 即 可 开 启 mac-auth-bypass。请注意,12.2(55)的 IOS 同时支持这两条命 令,但 12.2(25)/12.2(35)只支持 dot1x mac-auth-bypas eap 在实际使用时建议修改 tx-period 的值(思科默认为 30 秒),以缩短交换机重新发起认证的时间,使其尽快使用 mac 地址作为凭证认证。命令是:"dot1x timeout tx-period 5"。 2、H3C 交换机相关配置

与思科交换机不同的是, H3C 交换机配置 mac-auth-bypass时需要在 system view 和端口模式下分别 配置,其余基本一致。

在 system-view 模式下配置: MAC-authentication 和

MAC-authentication domain dot1x .

在接口下也要配置: MAC-authentication

## 无线网络准入配置



无线网络准入可支持标准 802.1x 用户认证,可信 mac 认证,可信 GUID 认证。

目前市面上大部分的无线路由器和AP基本上都支持802.1x准入的 设置,流程大致为:

1、客户端设置:在开始菜单的 venustech 目录中,选择无线置工具

📙 UltraISO	图片
📙 Unlocker	ARCENT OF A
📕 Venustech	音乐
J ESCC	
>> 天珣客户端	游戏
无线配置工具	计管机
🔜 修改Windwos防火墙设定	112400
📙 VMware	控制面板
📔 Windows Driver Kits	

并输入 SSID,点击设置并连接

局 无线配置工具			22
SSID 0	1 设置并连接	取消	
		422/1	

注: XP 系统下需要安装补丁 KB918997

- 2、 在无线路由器或 AP 上启用相应的 WPA/WPA2 认证;
- 3、在无线路由器或 AP 上配置天珣的 radius 服务器、端口及密码;

WPA/WPA2	
版本:	自动选择 👻
加密方法:	自动选择 👻
Radius服务器IP:	172. 25. 0. 226
Radius端口:	1812 (1-65535, 0 表示默认端口: 1812)
Radius密码:	123456
-	

**注意**: radius 服务器的密码与天珣 web 页面上配置的 radius 密码要 一致。

- 4、网络准入配置页面配置网络准入策略,并添加 radius 客户端设
  - 置, ssid 应填写无线路由器或 AP 的正确 ssid;



本页面设置无	线工作模式和参数。
SSID :	TP-LINK_AP
频 段:	5 🗸
模 式:	54Mbps (802.11g) 👻

2.换机能量				
交换机配置				
交換机名称	wlan			
立换机ip地址	172.25.0.249	*		
交换机品牌	D-Link	*		
交換机型号	DGS3200-10	-		
共享密钥	123456	*		
交換机类型	C LAN @ WLAN			
SSID	TP-LINK_AP			
动态VLAN支持	不支持		190	

- 5、无线信号经过无线路由器或 AP 时,会对其进行 802.1x 认证并 将认证信息转发给天珣 radius 服务器;
- 6、天珣 radius 服务器对认证信息进行认证,将认证完成的信息发 给无线路由器或 AP,然后决定是否对终端放行。

## H3C WX3024 无线局域网的相关配置 (瘦 AP)

## H3C WX3024 默认情况下 console 进入无线控制模块

## 无线控制器配置

[H3C]display current-configuration
#
version 5.20, Release 3110
#
sysname H3C
#
domain default enable dot1x
#
telnet server enable



```
#
 port-security enable
#
 dot1x quiet-period
 dot1x timer reauth-period 60
 dot1x authentication-method eap
#
 oap management-ip 192.168.0.101 slot 0
#
vlan 1
#
vlan 2
#
radius scheme dot1x
 primary authentication 10.201.7.1
 primary accounting 10.201.7.1
 key authentication 123456
 key accounting 123456
 user-name-format without-domain
 nas-ip 10.201.0.50
#
domain dot1x
 authentication lan-access radius-scheme dot1x
 authorization lan-access radius-scheme dot1x
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain system
```



```
access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
user-group system
#
local-user admin
 password simple admin
 authorization-attribute level 3
 service-type telnet
#
wlan rrm
 dot11a mandatory-rate 6 12 24
 dot11a supported-rate 9 18 36 48 54
 dot11b mandatory-rate 1 2
 dot11b supported-rate 5.5 11
 dot11g mandatory-rate 1 2 5.5 11
 dot11g supported-rate 6 9 12 18 24 36 48 54
#
wlan service-template 10 crypto
 ssid wlan_dot1x_test
 bind WLAN-ESS 10
 cipher-suite tkip
 security-ie wpa
 service-template enable
#
interface NULL0
#
```



```
interface Vlan-interface1
 ip address 10.201.0.50 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
interface WLAN-ESS1
#
interface WLAN-ESS10
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 undo dot1x multicast-trigger
#
wlan ap ap1 model WA2220E-AG
 serial-id 210235A42XB101000025
 radio 1
 radio 2
  service-template 10
  radio enable
#
ip route-static 0.0.0.0 0.0.0.0 10.201.0.1
#
 load xml-configuration
#
user-interface aux 0
user-interface vty 04
 authentication-mode scheme
```



user privilege level 3

idle-timeout 0 0

#

return

## 无线控制器对应的交换模块配置

<H3C>oap connect slot 0 进入交换模块

#
sysname H3C
#
oap management-ip 192.168.0.100 slot 0
#
radius scheme system
#
domain system
#
local-user admin
password simple admin
service-type telnet
level 3
#
vlan 1 to 2
#
interface Vlan-interface1
ip address 172.25.42.200 255.255.0.0
#
interface Aux1/0/0
#
interface GigabitEthernet1/0/1
#



interface GigabitEthernet1/0/2 # interface GigabitEthernet1/0/3 # interface GigabitEthernet1/0/4 # interface GigabitEthernet1/0/5 # interface GigabitEthernet1/0/6 # interface GigabitEthernet1/0/7 # interface GigabitEthernet1/0/8 # interface GigabitEthernet1/0/9 # interface GigabitEthernet1/0/10 # interface GigabitEthernet1/0/11 # interface GigabitEthernet1/0/12 # interface GigabitEthernet1/0/13 # interface GigabitEthernet1/0/14 # interface GigabitEthernet1/0/15 # interface GigabitEthernet1/0/16



# interface GigabitEthernet1/0/17 # interface GigabitEthernet1/0/18 # interface GigabitEthernet1/0/19 # interface GigabitEthernet1/0/20 # interface GigabitEthernet1/0/21 # interface GigabitEthernet1/0/22 # interface GigabitEthernet1/0/23 # interface GigabitEthernet1/0/24 # interface GigabitEthernet1/0/25 shutdown # interface GigabitEthernet1/0/26 shutdown # interface GigabitEthernet1/0/27 shutdown # interface GigabitEthernet1/0/28 shutdown #



## interface GigabitEthernet1/0/29

stp disable

port link-type trunk

port trunk permit vlan all

#

interface NULL0

#

user-interface aux 0

user-interface vty 0 4

authentication-mode scheme

user privilege level 3

无线控制器与交换模块之间通信说明:

无线控制器默认采用

interface GigabitEthernet1/0/1

port link-type trunk

port trunk permit vlan all

与交换模块

interface GigabitEthernet1/0/29

stp disable

port link-type trunk

port trunk permit vlan all

之间进行数据通信

## 胖 AP: WA2220-AG 配置说明:

```
<WA2220-AG>dis cur
```

#

version 5.20, Release 1113

#

sysname WA2220-AG



# domain default enable dot1x # telnet server enable # port-security enable # dot1x authentication-method eap # undo l2fw wlan-client-isolation enable # vlan 1 # radius scheme system primary authentication 172.18.18.70 primary accounting 172.18.18.70 key authentication 123456 key accounting 123456 user-name-format without-domain radius scheme dot1x server-type extended primary authentication 172.18.18.70 primary accounting 172.18.18.70 key authentication 123456 key accounting 123456 timer realtime-accounting 3 user-name-format without-domain undo stop-accounting-buffer enable #



# domain dot1x authentication lan-access radius-scheme dot1x authorization lan-access radius-scheme dot1x accounting lan-access radius-scheme dot1x access-limit disable state active idle-cut disable self-service-url disable accounting optional domain system access-limit disable state active idle-cut disable self-service-url disable # user-group system # local-user admin password simple 1231.xmccb authorization-attribute level 3 service-type telnet local-user venus password simple venus authorization-attribute level 3 service-type telnet # wlan rrm dot11a mandatory-rate 6 12 24 dot11a supported-rate 9 18 36 48 54



```
dot11b mandatory-rate 1 2
 dot11b supported-rate 5.5 11
 dot11g mandatory-rate 1 2 5.5 11
 dot11g supported-rate 6 9 12 18 24 36 48 54
#
wlan service-template 10 crypto
 ssid venustx
 cipher-suite tkip
 security-ie wpa
 service-template enable
#
interface NULL0
#
interface Vlan-interface1
 ip address 172.18.18.249 255.255.255.0
#
interface Ethernet1/0/1
#
interface WLAN-BSS10
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 undo dot1x multicast-trigger
#
interface WLAN-Radio1/0/1
#
interface WLAN-Radio1/0/2
 service-template 10 interface wlan-bss 10
#
```



ip route-static 0.0.00 0.0.00 172.18.18.254
#
arp-snooping enable
#
load xml-configuration
#
user-interface con 0
user-interface vty 0 4
authentication-mode scheme
#
return

# 6.3. 应用准入

## 6.3.1. 关于应用准入

- "应用准入":采用多种策略网关,为企业的关键信息系统和应用提供准入控制手段。只有受天珣管理并且符合安全策略的电脑才允许访问企业的这些系统及应用。应用准入控制为企业关键信息系统提供安全保护,杜绝非授权访问和非安全访问。
- 策略服务器(中心服务器或本地服务器)只与策略网关代理 通讯。在有多个策略网关的环境下,这样的机制能极大简化 配置。
- 策略网关代理代替策略网关确认终端是否已安装天珣客户端,当客户端主动退出后,策略网关代理负责通知各策略网关及时拦截该终端访问策略网关。
- 这种机制同样可以跨越负载均衡设备,只需负载后面的设备



单向链接到策略网关代理即可,而不需要负载后面的网关与 客户端双向通信。

下图是策略服务器、策略网关代理和策略网关的关系示意图:







下图是应用准入工作流程示例图:





## 名词解释

策略网关代理:策略网关代理代表一组策略网关对终端安装天珣客 户端认证与安全状态确认。这些策略网关应该具有相同的准入控制 需求。在策略配置时,将这一组策略网关作为一个管理对象来管理。 一般情况下,一个企业需要做准入控制的网段是统一的,即哪些终 端需要安装天珣客户端,哪些终端不必须安装天珣客户端。根据公 司实际环境,这些准入范围是已知的,只需要配置一个策略网关代 理即可。

但也有特殊情况,比如某公司的分支机构有一个专用服务器,该服 务器仅需要给该分支机构的几千人提供服务。在此服务器上安装策 略网关就不需要连接至总部的策略网关代理了。此时可以新建一个 策略网关代理,其准入控制网段仅仅是该分支机构的 IP 组范围。

**"策略网关"**:即安装在应用服务器上的准入服务程序,策略网关 连接至策略网关代理取规则并对访问的终端作安全检查。

天珣支持的应用准入策略网关类型有:

按应用系统分类:Web、Mail、DNS、ISA 代理。

按操作系统分类: Windows、Linux。

下表是天珣具备的针对不同业务应用的策略网关类型列表,用



户总可以从中找到一种或几种适合自己业务应用的应用准入控制 解决方案:

网关类型	不同平台下可发	选择的策略网关
应用类型	Windows	Linux
Web 应用	IIS 策略网关	中性(通用)策略网关 for Linux
Proxy 应用	ISA 策略网关	中性(通用)策略网关 for Linux
DNS 应用	中性(通用)策略网关 for Windows	中性(通用)策略网关 for Linux
其他应用类型	中性(通用)策略网关 for Windows	中性(通用)策略网关 for Linux

表 3 天珣针对不同业务应用的策略网关类型列表

除此之外, 天珣能够与启明星辰天清汉马一体化安全网关(简称: 天清汉马 USG) 联动, 实现准入控制互动, 由天清汉马 USG 担当准入控制网关, 当计算机终端需要通过天清汉马 USG 进行访 问时, 由天清汉马 USG 和天珣联动, 确保只有安装天珣客户端程 序、接受天珣管理并且符合企业安全策略的计算机终端才能通过天 清汉马 USG 进行访问。

天珣还能针对一些特定的第三方 web 应用来实现 web 准入控制。这种准入控制方式没有特定的操作系统要求,只需将嵌入代码写入 web 登录页面的源代码中,由嵌入式代码检查发起访问的客户端 IE 是否安装了天珣的 IE 控件,并由此 IE 控件和天珣服务器一起决定此客户端是否能够正常访问该 web 页面,从而达到准入的目的,确保只有安装天珣客户端的终端才能安全访问。

天珣应用准入控制可以单独只启用一种平台进行应用准入控制,也可以同时启用多个平台进行应用准入控制,也可以与网络准入控制同时启用,组成"网络准入+应用准入"的复合准入控制体系。 更可以与启明星辰天清汉马一体化网关进行准入控制联动,通过多种准入控制手段的组合,全面覆盖企业内网每一个区域和角落,有效保证计算机终端始终安装天珣客户端程序并接受天珣管理。



## 6.3.2. 策略网关代理设置页面

配置介绍

<b>机制料关代</b> 提	¥						
策略网关作	建衰量 📑	i hu					
用关终带	176.9	<b>Baska</b> ak	东京学校内设	kiit k	NEFA	<b>S</b> Ø.	法教给室唱用关
the second s		- Margaretter	PRO- NAME OF A	Constant Sec.		The statement of the state	

点击"应用准入"配置页面,将看到策略网关代理设置结果如上图。 策略网关信息页面

点击"连接的策略网关"查看链接,可以看到当前策略网关代理连 接的策略网关信息。

策略网关代理设置	
策略网关代理[192.168.1.16]管理的策略网关	返回
策略网关IP	策略网关类型
192. 168. 1. 16	中性策略网关
192. 168. 0. 2	VSG

注意:如果某策略网关并没有在此页面中显示,说明该策略网关并没有正确连接至策略网关,问题可能出在策略网关端或者是网络端口不通。端口为由策略网关单向连接至策略网关代理的 tcp 7893,请检查网络配置。

## 配置策略网关代理页面

点击**策略网关代理**名称,可进入策略网关代理添加\配置页面



略两关代理设置		
146元天代徽名称	開始同天代建	
198.32	10.201.1.204	<u> </u>
(原稿)法	初始的繁新四天代谢	2
		-1
議的管理阿根	10, 201, 1, 204	2
求刘方策略成本	050101000	中心服装翻架唱歌半: 110914075
证客户属是管理延安全状态	P THE	
证等户确是否确是学生状态	作不動徒 C 安全状态完整时取得,不完整 C 安全化本产型时取得,不完整	T给出城子后放行
业等户端是古典社学圣状态 户端下载地址	※不能は へ安全状态気能付取り、不気数 へ安全状态気能付取り、不気数 「安全状态気能付取り、不気数 「新たり//10.201、1.204:8835/1	17%出版子-系统订 1%出版子-系统门 10%10ad/C1
证客户编基古典社安坐状态 户端下载地址 理员能名	※ 不動達 C 安全はあれ最終的で、不太数 C 安全はあれ最終的で、不太数 Datap://10.201.1.204:8835/1 間望然	町輸出調子-転数行 町輸出調子-転数行 IamiLoad/CI
让客户编唱古教社安全状态 户端下载地址 塑质地名 運動电话	※ 不動使 C 安全なお売期付款()、不売期 C 安全なお売期付款()、不売期 [http://10.201.1.204:88335/ 管理員	9%出现子-后约订 9%出现于后下的门 10%10ad/C1
2. 20 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	※ 不動達	9%出版子系的订 9%出版子系不依何 formIcad/CI
记者户属是古典社会全状形 学员地名 学员地话 学员他们在过 用个性化客户编辑子页面	<ul> <li>※ 不動使</li> <li>※ 安全なお天殿村取行, 天天殿</li> <li>ぐ ※ 安全な天殿村取行, 天天殿</li> <li>「 ※ 安全な天殿村取行, 天天殿</li> <li>「 「 「 」</li> <li>「 「 」</li> <li>(1) (1) (2) (1) (1) (2) (1) (1) (2) (1) (1) (2) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1</li></ul>	19後出議デ系数で 9時出議デ系下数で 1999-1994/CI

- 雅戶·國始的5並入這後 是言曲用1853並入	<ul> <li>不成用</li> <li>2) 対所有005勝方環気法の清末成用005まえ、</li> <li>2) 役23以下005勝方環気法的清末成用005まえ、</li> <li>2) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1</li></ul>
解释应用对象	<b>煮</b> 有及用油
创建状态	28
创造典	administrator
主+石边青+马的项目企须输入+	
	(17.77) MIDE 40.76

配置项:	说明
策略网关代理名称	标记该策略网关代理的名称,方便日常管理。
IP 地址	策略网关代理的 IP 地址,告知中心服务器该策略网关 代理的 IP 地址,提供策略网关代理的准入策略。
网段描述	方便日常管理,非必填项。
所属的管理网段 关代理如何取策略。	
要求对方策略版本 用于强制客户端更新客户端版本。如果某客户端规本低于指定的规则版本,策略网关将强制阻断访问	
验证客户端是否满	主要有三种验证方式:(1) <b>不验证</b> ;即不对客户端的安



足安全状态	全状态做任何验证,就算客户端的安全状态不满足,也
	不会弹出任何提示;(2) 安全状态完整时放行,不完整
	时给出提示后放行;当客户端的安全状态不完整时,会
	弹出提示框,但是网络依然是通的;(3)安全状态完整
	时放行,不完整时给出提示后不放行;当客户端安全状
	态不完整时,会弹出提示框,本次连出被拒绝。
	客户端下载提示页面中客户端的下载地址,默认选项即
客户端下载地址	म्रे °
	如果客户端下载 URL 非默认,则可以在此处更改。
管理员姓名	管理员名称,提示页面会有显示。
管理员电话	管理员电话,提示页面会有显示。
管理员邮件地址	管理员邮件地址,提示页面会有显示。
	如果默认提示页面不能满足用户要求,可由用户自定义
启用个性化客户端	提示页面。该提示页面可以是独立的 web 站点, 甚至可
提示页面	以是独立的 WEB 服务器。此时需要选择"启用个性化客
	户端提示页面"。
坦二百元 IDI	个性化提示页面的 url。该提示页面可以是任意 url,
远小贝面 UKL	比如:有天珣客户端下载链接的公司门户网站。
	有三个选项:(1)" <b>不启用"</b> ,当不启用 DNS 准入时,则
	勾选此选项;(2)对所有 DNS 服务器发送的请求启用
客户端 DNS 准入选	DNS 准入;(3) 安全状态完整时放行,不完整时给出提
项	<b>示后不放行;</b> 当要启用 DNS 准入时,则勾选第二、三
	选项,还有,要记得在 <b>中性策略网关配置</b> 里面把"启用
	DNS 检查"也勾选上,默认是不勾上的。
策略应用对象	即该策略网关代理将对哪些对象做准入控制

**注意**:如果策略网关、策略网关代理、中心服务器分别在不同的服



务器上,此处需要填写的 IP 地址是策略网关代理的 IP 地址。

**注意**:如果网络中网段很多时,特别注意策略网关代理所在的管理 网段,注意选择正确的管理网段。

**注意**:如果启用了个性化提示页面,天珣策略系统默认提示页面的 所有配置信息将失效。

#### 策略应用对象页面 策略网关代理设置 策略网关代理 对象类型 IP组 全部选中 Ŧ 对象选择 工作组 🔲 110 📝 99100 🔲 10.201.1 主机名 172.25.1 🔲 140 254 🗖 172.25.85.1 🔲 172.25.22.X 确定 取消

可以应用到 IP 组,工作组,主机名。

**注意**:当前版本中若要排除某 IP 地址不做准入控制检查,不能为 该 IP 地址添加独立的 IP 组并取消准入控制。而需要在 IP 组中添 加该 IP 地址的例外排除。



IP组				
卫雄名称	172.25.100.*			
卫坦斯地	172, 25, 100, *			1
所屬的服务器	CenterServer			1
所屬的管理同時	1004488			1
本口组中的口地址	2.6	FREEK	经交通社	-
	172, 25, 100.*	172 25 100 1	172.25.100.255	
排除的地址		1110.00		511 BZ
	172.25.100.254			単加
Sector and				
the second se				

不建议单独 IP 地址做准入控制检查,否则容易导致配置逻辑混乱。 例如: 192.168.0.0/24 网络,测试时仅有一台客户端做测试,建 议先添加一个 ip 组,该 IP 组的范围是 192.168.0.0/24,并对该 ip 组做准入控制和 MAC-IP 绑定。而客户端具体功能测试可以单独 建立一个单 ip 地址的 IP 组。

### 配置要点

- 1、点击"添加"策略网关代理设置;
- 2、输入"策略网关代理名称"、策略网关"IP 地址"、配置管理员 信息;
- 3、点击"策略应用对象"中"查看及编辑"超链接,选择需要准 入的类型并确认;
- 4、保存策略网关代理配置页面后,即时更新策略网关规则。

**注意:**确认策略网关代理的 IP 地址在管理网段中,否则策略网关 代理无法获取准入规则,导致应用准入功能失效。

## 6.3.3. 中性(通用)策略网关安装配置要点

1、请点击"安装中性(通用)策略网关"运行中性(通用)策略网关的

setup 程序,一步步按照提示进行安装。





2、安装结束之前,请注意阅读下面的重要信息。



3、安装完成后,中性(通用)策略网关配置程序启动进行驱动、端口检查、可忽略检查 IP 的配置。

4、配置中性(通用)策略网关驱动程序。首先安装驱动程序,当驱动程序已经安装时,"安装驱动"按钮不可用。安装完驱动程序后,驱动默认对所有的网卡进行监控。如果运行中性(通用)策略网关的机器上有多块网卡,需要将不直接与 CC 客户端通讯的网卡选择状态改为不选中,然后点击"应用网络配置"按钮使配置生效。



	E BERNING	
Fraising	PHR社	Franklin
MMDIAn Force Networking Controller MMDIAn Force Networking Control Intel(R) PRO(1000 MT Network Co 図 WAN 教動論ロ (P)	192.168.99.33 0.0.0.0 10.33.1.217	(1a3e05be-1e45-494b-9174-d7385 (1a3e05be-1e45-494b-9574-d7385 pdiven_80868dev_1076 ms_ndswanp
· · · · · · · · · · · · · · · · · · ·	200	214

5、配置中性(通用)策略网关使用的策略网关代理地址、监控 TCP 端口的范围以及可忽略检查的 IP 地址。程序默认监控 80 和 8080 端口。

繁彩的关代理	Ptett: 10 .	33 . 1 . 217	保存	
Dallanden 🖪	金麦端口花瓶配置	STREND HALL DER CONSIS	<b>查配谱</b>	
龙柏梁口	接來讓口	第四说明		
8080	80 8090			

6、点击保存,完成中性(通用)策略网关配置。

7、如果需要启用 DNS 准入功能,请将中性(通用)策略网关安装在 DNS 服务器上(旁路 DNS 准入无需安装在 DNS 服务器上),并在 中性(通用)策略网关配置界面中,进入 DNS 检查配置选项,勾选 启用 DNS 检查,勾选后默认 DNS 服务器将启用准入检查,对所有 来访的 DNS 请求进行检查。假设想对某些域名进行例外排除,可 以在"例外的域名"栏中填入相应的域名并"添加"即可。



第略同关代理中能址: 10	, 33 . 1 . 217	保存	
网络舰动和管门检查端口范围和管	t   Statutet (DV	杨重配版	
₩ 启用ows检查			
\$19930942.01		港加	
资外的域名列表			
		BR	

8、安装配置成功后,请进入服务控制器,若系统已经自动添加"ES GatewayPlugin Service"服务,则表明策略网关代理已经安装配置 成功。注意此服务第一次需手动启动,以后则可以自动启动。 9、参考<u>《应用准入-配置要点》</u>.

## 6.3.4. 旁路 DNS 准入

DNS 策略网关不单支持在内部 DNS 服务器上安装部署,实现对 DNS 服务器的检查和控制,也支持在没有内部 DNS 服务器的环境 中对终端进行 DNS 请求的检查和控制。假如安装在内部 DNS 服务 器上策略网关将自动按照在线服务模式(Pass Through)执行 DNS 应用准入,实现旁路侦听和在线服务模式自适应自动切换,满足各 种网络环境下,实现基于 DNS 应用的客户端准入控制。 下图为工作在旁路侦听模式的新 DNS 策略网关部署逻辑图:





- a) 在用户使用的 DNS 服务器不统一的情况下,建议将新 DNS 策略 网关连接在互联网出口交换机的镜像监听端口上;
- b) 客户端的 DNS 请求包经过出口交换机时,会被完整复制一份到 镜像监听端口,并由策略网关检查其是否安装天珣或是是否合 规;
- c) 也可以直接使用 HUB 接入策略网关, HUB 上连接的其他终端都 将直接受到监听而无需设置镜像;
- d) 可选择任意一台服务器作为 DNS 应用准入服务器,此服务器上可以不装任何其他应用服务,例如 IIS 等等;

在设置交换机端口镜像时,不要把端口所有的数据都镜像,这样会造成监听口网络流量巨大,可能造成网络阻塞,只需要对 DNS 请求数据镜像就行;



## 6.3.5. IIS 策略网关安装配置要点

1、请点击"安装 IIS 策略网关"运行 IIS 插件策略网关的 Setup 程 序,一步步按照提示进行。

700 天动内网安全风	险管理与审计系统
安装策略网关	
前当场大关机器的其他两大。	安装策略阿夫代理
	安装中性策略网关
	安装15策略同关
	安装ISA策略两关
	安装EXCHANGE策略同关
	<b>赵国</b>

2、进入策略网关控制面板,设置策略网关代理 IP,点击"保存"。

策略网关控制面极	
策略网关代理IP	192. 168. 0, 236
	保存
安裝ISA防火墙插件	卸载ISA防火墙插件
安裝ISA代理插件	卸载ISA代理插件
安裝SMTP邮件插件	卸载SMTE邮件插件
	关于

3、打开 Internet 服务管理器, 右击"默认 Web 站点", 打开"属性"

## 配置。

4、在 ISAPI 筛选器属性页下,增加一个筛选器。



简改基属性		×
筛选器名称 (2):	epol	
可执行文件(2):	C:\WINNT\system32\i	inetsrv\filter\is
		(MR B)
确定	取消	帮助(H)

5、为筛选器输入一个名称,可执行文件为

"WINNT\System32\Inetsrv\filter\isawebfilter.dll"。

6、重新启动 IIS 控制服务和 World Wide Web 服务,插件就已经生效。

7、参考《应用准入-配置要点》。

## 6.3.6. ISA 策略网关安装配置要点

- 1、天珣内网安全风险管理与审计系统提供分别适用于 ISA2000 和 ISA2004 的两种策略网关。
- 2、请点击"安装 ISA 策略网关",进入安装 ISA 策略网关的选择 界面。

700 天珀内网安全风	险管理与审计系统
安装策略网关 语选择实装相应的策略网关。	安装策略同关代理
	安装中性策略网关
	安装IIS策略同关
	安装ISA策略网关
	安装EXCHANGE策略同关
	<b>王</b> 王王王王王王王王王王王王王王王王王王王王王王王王王王王王王王王王王王王

- 运行相应的 ISA 插件策略网关的 Setup 程序,一步步按照提示 进行安装。
- 4、 点击"安装 ISA 防火墙插件",注册 ISA 防火墙插件。




5、如果插件注册时报告错误,主要可能的原因是注册进程的权限 不能满足管理 ISA Server 的需要导致。可先尝试在插件安装目 录(ISA 安装目录\Filter)下运行

#### Regsvr32 /i:array ISAAPPFilter.dll

- 6、如果还是出现错误,尝试打开 ISA 管理控制台,看当前用户是 否可以修改 ISA 配置。
- 7、 点击"安装 ISA 代理插件",注册 ISA 代理插件。

	策略网关代理IP	192. 168. 0	0. 236	<u> </u>	1	
			Ţ	保存		
0#32						
ovr32	legisterServer in CúDrog	ram Eilec' Micro	coft ISA Se	wuari Eiltar	TEAWabE	ilter
	tegisterServer in C:\Progi ceeded.	ram Files\Micro	soft ISA Se	erver\Filter	ISAWebF	ilter.
	legisterServer in C:\Prog ceeded.	ram Files\Micro 備定	soft ISA Se	erver\Filter	ISAWebF	ilter.
	egisterServer in C:\Prog ceeded.	ram Files\Micro	soft ISA Se	erver\Filter	ISAWebF	ilter.

8、如果插件注册时报告错误,主要可能的原因是注册进程的权限 不能满足管理 ISA Server 的需要导致。可先尝试在插件安装目 录(ISA 安装目录\Filter)下运行

#### Regsvr32 ISAWebFilter.dll

- 9、如果还是出现错误,尝试打开 ISA 管理控制台,看当前用户是 否可以修改 ISA 配置。
- 10、 在 ISA 插件安装目录下有一个 ISAWebFilter.ini 文件,通 过该文件可以配置当用户通过 WebProxy 访问某些站点时不需



要检查客户端是否满足要求。

- 11、 重新启动 ISA 的 WebProxy 服务和 Firwall 服务,插件就 开始运行。如果插件启动时策略网关代理没有运行导致插件取 不到规则,插件会每隔 30s 重新连接策略网关代理。
- 12、 完成安装注册后,请进入 ISA 控制器,检查在 Extensions 选项下的 Application Filters 中的 EPolHTTPFilter 以及 Web Filters 中的 Web Filter 是否正常启动,如正常则 ISA 策略网关 安装注册成功。



- 13、 如要卸载插件,点击"卸载 ISA 防火墙插件"或"卸载
   ISA 代理插件"。
- 14、 参考《应用准入-配置要点》。



# 6.3.7. Exchange 策略网关安装配置要点

 1、请点击"安装 Exchange 策略网关"运行 Exchange 插件策略网 关的 Setup 程序,一步步按照提示进行安装。



2、安装完成点击进入策略网关控制面板

策略网关代理IP	192.	168.0.236	
			保存
安裝ISA防火墙插件		卸載IS	城火墙插件
安裝ISA代理插件			SA代理插件
安装SMTP邮件插件	Ĩ	卸载SM	TP邮件插件

3、 点击"安装 SMTP 邮件插件",注册邮件插件。



	策略网关代理IP	192.16	8.0.236			
				保存		
	19 <b>-</b>					
a 32						
) E:	\WIN2003\system32\EP	olEx\EPolE:	x.DLL 中的	DllRegi	sterServer	,成
) E:	\WIN2003\system32\EP	olEx\EPolE:	x.DLL 中的	DllRegi	sterServer	r 咸
) E:	\WIN2003\system32\EP	olEx\EPolE	x.DLL 中的	DllRegi	sterServer	r pţ
) E:	\WIN2003\system32\EP	olEx\EPolE: () 研定 王)	x.DLL 中的	DllRegi WITAIT	sterServer	- ज़

- 为该插件配置合适的插件规则,重新启动 Exchange 服务,插 件就已经生效。
- 5、安装注册完成后,请点击"开始"→"程序"→"Venus"→"邮件插件策略网关"→"邮件插件状态查看",若状态为"激活"则表明 Exchange 策略网关安装配置成功。
- 6、如要卸载插件,点击"卸载 SMTP 邮件插件"即可。
- 7、参考《应用准入-配置要点》。

## 6.3.8. Web 准入安装配置要点



1、在 web 页面源代码中嵌入天珣 activex 控件代码,以 asp 为例:

<form action="index.asp" method="post">

username:

<SCRIPT language=javascript>



function DetectWebCheckerActiveX(){

```
try
{
```

var comActiveX = new

ActiveXObject("WebChecker.WebCheckerTextbox.1");

```
}
catch(e)
{
    return false;
}
return true;
};
```

if(DetectWebCheckerActiveX()==true){

document.write('<OBJECT id=WebCheckerTextbox

codeBase=http://172.25.9.11:8833/Download/WebChecker.cab#versio

```
n=1,0,0,1
```

classid=CLSID:51EA9310-CE77-4D0F-99FF-6CD8017AFBC4><PA

```
RAM NAME="ProxyIP" VALUE="172.25.9.11"><PARAM
```

NAME="width" VALUE="4000"><PARAM NAME="height"

```
VALUE="500"></OBJECT>');
```

}

else{

document.write('<a

href="http://172.25.9.11:8833/Download/WebChecker.exe">请点此下 载控件</a>'); } function GetText(){

var data;

data = document.getElementById ("WebCheckerTextbox").GetTextValue

();



```
document.getElementById("UserName").value = data;

}

</SCRIPT>

<br />

usercode:

<input type="text" name="Code"/>

<br />

<br />

<input type="hidden" name=wd id="UserName" value="dhhh"/>

<input type="submit" value="提交" onclick="GetText()"/>

</form>

<%

Response.Write(Request.Form)

%>
```

2、没有安装 web 准入控件的终端访问此服务器时, 会提示下载并 安装控件:

| 登录                   |                        | ×                |
|----------------------|------------------------|------------------|
| R                    |                        | 1 Th             |
| 登录名:<br>密 码:<br>校验码: | <u>请点此下载控件</u>         |                  |
|                      | 0 3 4 <u>看不清</u><br>登录 | <u>,再选一张</u><br> |

3、点击"**请点此下载控件"**,下载安装控件即可:





4、安装完成后将正确显示登录界面:

| 登录   | ×           |
|------|-------------|
|      | 5.0         |
| 10   | Joseph Land |
|      |             |
| 登录名: |             |
| 密码:  |             |
| 校验码: |             |
|      | 6 5 7       |
|      | 看不清,再选一张    |
|      | 登录    重设    |

5、正常登录后,如果终端本身没有运行天珣客户端,则在访问页 面时会弹出跳转提示页面要求用户安装天珣客户端;如果安装 了天珣客户端但安全基线不满足要求的话,则会在登录框中提 示终端不合规:

| 登录   | ×                       |
|--|-------------------------|
| The second secon |                         |
| 登录名:<br>密 码:   | 天珣提示终端不合规               |
| 校验码:   | 5016<br><u>看不清,再选一张</u> |
|  | 登录重设                    |



# 6.4. 客户端准入

# 6.4.1. 关于客户端准入

- 客户端准入有两层含义:一是接收到访问请求时,检查对方是 否安装天珣客户端,同时检查自己是否符合安全策略;二是客 户端访问网络时,要检查自己的安全状态是否符合策略。
- 客户端准入启用时注意将无法安装天珣客户端的终端做例外 排除。例如:远端网段为同一子网时,同一个子网内的网络打 印机、交换机、Linux 服务器等。远端网段为全部管理网段时, 全部管理网段内的 web 服务器、dns 服务器、OA 服务器等等。
- 在启用了客户端准入控制的终端上,点击防火墙对话框的"查 看全局策略设置",可以明确查看客户端准入控制策略,而且 该策略前有明确的标识为客户端准入策略,以方便管理员日常 管理。
- 客户端准入的准入类型为连出时,远端网段为所有地址。启用 后的效果为:"满足安全基线时放行,不满足时拒绝并给出提 示"。

**说明:**来访的终端的安全状态是由来访终端自己检查的,如果不符 合安全策略客户端将自动拦截访问连出。但实际的效果等同于客户 端A检查了客户端B的安全策略是否满足。

下图是客户端准入控制示意图。





### 名词解释

**客户端准入:** 安装有天珣客户端的终端发出的 IP 包将具有天珣特征标志。对端客户端接受到该 IP 包时如果发现该 IP 包没有天珣特征标志,则拒绝接受该包。实际的效果为未安装天珣客户端的电脑将无法访问已安装天珣客户端的终端。

建议: 客户端准入连入检查的范围一般为同一子网。

## 6.4.2. 客户端准入页面

### 配置介绍

| 客户蕹准入                          | 添加  |         |         | 1      |
|--------------------------------|---|---------|---------|--------|
| 1002#                          | TREF  | 对这次表行某人 | 间在黑星行星入 | 网络阿拉克博 |
| 國一部局的國際的基本的<br>臺內國的科学社会的基本的    | 相互解解。用一子同的首曲电路<br>高速行業の編約日子には高速を<br>低。高期本利用は近方的約月子<br>子明記。主意行業にから作<br>後。              | 1       | a.      | 两开闩    |
| <u>本化中的石油已至今期往</u> 十<br>计论改进问题 | 社園策略,本机和蘇泰萬空安全<br>重統才行為访问单位內對列級,<br>互加於均等維持時,希維出還<br>市。主意何爾匹子/加特於,并<br>主访问事单位阿線了不预算制。 | đ       | #       | 282976 |



| <u>客户端准入</u> |   |
|--------------|---|
| 客户端准入        |   |
| 策略名称         | 同一子网的其他电脑演运行客户端软件才允许1+  |
| 策略描述         | 预置策略。同一子网的其他电脑须运行客<br>户端软件才允许访问本机。否则本机将对<br>对方的访问不予响应。注意仅限TCP/000协  |
| 准入类型         | <ul> <li>ジェン(透漏回版的电脑质语行客户编软件目本编要满足安全状态才允许连入)</li> </ul>   |
| 远端阿根         | <ul> <li>二 査出(本備电話演員上安全状态才允许访问這個问程)</li> <li>※ 同一子网</li> </ul>  |
| 例外的IP地址      | ◎ 全部管理网级  |
| 主动时间         | ※     ※     ※     ※     ※     新育时頃 ○ 工作时间 ○ 車工作时间 ○ 以下时间段     市公司 所     がまり     かり     か |
| 在线模式         | ◎ 在线时生效 □ 高线时生效   |
| 策略应用过象       | (还没有应用到任何对象) <u>查看四课题</u>   |
| 创建类型         | 全局  |
| 创建会          | jing  |
| 注:右边有+号的项    | 日必须输入。<br>保存 翻錄 取消  |

| 配置项: | 说明   |
|------|--|
| 策略名称 | 用以标示策略,方便管理。例如:财务部客户端准<br>入(连入)  |
| 策略描述 | 财务部终端只允许接受安装天珣客户端的终端访问。  |
| 准入类型 | 准入类型分连入和连出两个方向。如果选择连入,<br>则天珣客户端对连入的访问确认是否可信,如果连<br>入终端未安装天珣客户端或者受访终端不满足安<br>全基线时,则将被拒绝访问。如果选择连出,则本<br>地访问网络时客户端检查本机安全基线如果安全<br>基线符合策略,允许访问;如果安全基线不符合策<br>略,拒绝访问并提示。 |
| 远端网段 | 同一子网指天珣客户端仅检查远端网段属于同一<br>子网的终端是否有安装天珣客户端,对于子网外的<br>访问一律放开,例如:服务器区的 dns、dhcp 广播<br>信息等。建议客户端准入选择此模式。该模式下远<br>端网段例外排除的 IP 地址将容易配置;                                     |



|   |               | 全部管理网段指对策略服务器配置的所有管理网       |
|---|---------------|-----------------------------|
|   |               | <br> 段内均启用客户端检查。该种模式的客户端检查需 |
|   |               | 要跨越子网,因此需要例外排除的 IP 地址将需要    |
|   |               | 详细进行配置。                     |
|   |               | 远端网段默认是同一子网。                |
| Ĭ |               | 在客户端检查子网范围内对指定的 IP 地址作例外    |
|   | 远端网段例外的 IP 地址 | 排除,需要排除的 IP 地址包括:网络打印机、无    |
|   |               | 法安装天珣客户端的终端、DNS 服务器等。       |
| I | 在线模式          | 客户端准入仅在天珣客户端在线时生效,不存在离      |
|   |               | 线模式。此处不可选择。                 |
| I |               | 选择哪些 IP 组,工作组或主机名的终端需要启用    |
|   | 東略应用对象        | 客户端准入。                      |
|   |               | 1                           |

**注意:**客户端准入检查的网络访问行为是所有的 tcp/udp 网络行为, 但不包括天珣策略系统端口。

**注意**:另外,天珣防火墙特有的机制决定了启用客户端准入时,对 已经建立的网络连接将仍保存放行。

#### 配置要点

- 1、点击"添加客户端准入"建立连入策略;
- 2、准入类型选择"连入(远端网段的电脑须运行客户端软件才允 许连入)","远端网段"选择"同一子网";
- 3、排除该子网内的网络打印机、网络复印机等 IP 地址;
- 4、点击"策略应用对象""查看及编辑"超链接,选择应用类型 及终端,保存退出;
- 5、点击添加"客户端准入",建立连出策略;
- 6、准入类型选择"连出(远端网段的电脑须运行客户端软件才允



许连出)","远端网段"选择"全部管理网段";

- 7、排除杀毒软件服务器、补丁服务器、安全修复下载服务器等 IP 地址;
- 8、点击"策略应用对象""查看及编辑"超链接,选择应用类型 及终端,保存退出。

# **6.5.** ARP 准入

## 6.5.1. 关于 ARP 准入

- ARP 准入,是由受控的终端使用异常的 ARP 数据包,阻断和
   干扰非受控的终端的网络连接,从而达到终端网络准入控制的
   目的。
- 为了使 ARP 准入生效,在1个 IP 子网内,至少要在1台终端 上安装天珣客户端(受控终端)。
- 未安装天珣客户端的终端(非受控终端)发出的 ARP 请求, 将会收到受控终端发出的异常的 ARP 应答包,从而使非受控 终端与其他终端不能正常通信。对于已安装天珣客户端的终端 (受控终端)发出的 ARP 包,其他受控终端不发异常 ARP 应 答包。
- ARP 准入是基于网段启用的,您必须为每个子网(广播域)
   配置一条 ARP 准入规则。





# 6.5.2. ARP 准入页面



| 配置项:       | <u>说明</u>                                       |
|------------|---|
| 子网         | 启用 ARP 准入的子网的网络地址,比如192.168.100.0。              |
| 子网掩码       | 子网对应的子网掩码,比如 255. 255. 255. 0。                  |
| 网关1的 IP 地址 | 无论网关是否安装了客户端,受控终端始终不对<br>其实施 ARP 欺骗。可以设置两个网关地址。 |



| 网关 2 的 IP 地址 | 无论网关是否安装了客户端,受控终端始终不对<br>其实施 ARP 欺骗。可以设置两个网关地址。 |
|--------------|---|
| 不限制的 MAC 地址  | 无论这些 MAC 地址对应的终端是否安装了客户端,受控终端始终不对其实施 ARP 欺骗。    |

注意:因天珣客户端不会对默认网关回应错误的应答,所以不会影 响受控终端访问网关。这样也带来了非受控终端在一定的时间段内 是可以访问外网的现象。反之,如果发现网络中默认网关有多个 MAC 地址,(而这些 MAC 地址不是网关设备的特殊配置),网络 可能存在 ARP 欺骗,这种欺骗行为不属于天珣客户端准入行为。 如果某终端被 ARP 欺骗,而该终端却没有任何错误应答包,则该 欺骗不是天珣客户端的准入行为。

**注意:** 开启 ARP 准入需要特别谨慎,建议仅作为其他准入方式的 一种补充。

#### 配置要点

- 1、输入子网号,例如: 192.168.0.0;
- 2、输入子网掩码,如:255.255.255.0;
- 3、输入网关1的IP地址,如:192.168.0.1;
- 4、 排除网络打印机的 MAC 地址或其他重要的服务器地址;
- 5、保存,客户端更新策略,ARP准入策略生效。



# 7.安全防护

# 7.1. 关于安全防护

- 通过天珣内置的进程级访问控制内核,可以实现针对终端基于进程、端口或协议的双向访问的最细粒度的访问控制;有效管理终端带宽,并通过监控TCP及UDP的连接,对异常流量进行控制,对ARP欺骗进行有效的控制。
- **服务:**服务即终端机器的端口或协议,管理员可针对服务类型(端口和协议)配置有效的访问控制策略。
- **服务组**:多个服务的集合。
- 服务器地址:可以添加一个远端访问的服务器 IP 地址。
- **自定义网段**:用户可以自定义一个远端访问的 IP 网段。
- 访问控制:对客户端的连入和连出访问进行控制,可控制客 户端只能访问许可的地址,只能访问许可的服务,只能由指 定的程序访问等。可针对进程、端口及协议进行详细的订制。
- 流量控制:利用分布式带宽管理每个终端上的每个应用程序,每个端口的流量和带宽。通过合理配置,能有效管理终端的异常流量,即使出现突发状况,也能保证网络正常业务访问。
- **攻击防护:**通过对终端TCP和UDP的连接及发包数量的监控, 保护终端不受攻击,并通过监控ARP请求和应答,防止内网 ARP欺骗的发生。
- PING 控制:对客户端的 ping 出和被 ping 进行控制
- 访客策略:对于任何网络准入类型(标准 802.1X 和漫游网段的 802.1X),如果基本认证的认证方式为可匿名的用户认证,则在登录成功后获取防火墙访客策略。此时可设置访客策略为最小访问权限,保证内网安全。



# 7.2. 协议端口设定

## 7.2.1. 配置介绍

协议端口设定是服务、服务组及服务器地址和自定义网段的一个 集合。通过这些定义的配置增加策略设置的灵活性。

### 服务

服务是 TCP/IP 的协议和端口的组合,比如 SMTP 服务是 TCP 协议 和 25 端口的组合,DNS (UDP) 协议是 UDP 协议和 53 端口的组合。 系统安装时已经配置了最基本的一些服务。

点击"**服务**",系统显示目前已经配置的服务(包括预置的服务)。

| ervice 添加         |     |                 |
|-------------------|-----|-----------------|
| 3称:               | 端口: | 查询 邦助           |
| <u>Service名称</u>  | 协议  | <u>市场</u><br>端日 |
| 不限                | 不限  | 不限              |
| echo (7)          | 不限  | 7               |
| discard(9)        | 不限  | 9               |
| systat (11)       | 不限  | 11              |
| daytime (13)      | 不限  | 13              |
| gotd (17)         | 不限  | 17              |
| chargen (19)      | 不限  | 19              |
| ftp-data(20)      | TCP | 20              |
| ftp(21)           | TCP | 21              |
| <u>ssh (22)</u>   | TCP | 22              |
| telnet (23)       | TCP | 23              |
| smtp(25)          | TCP | 25              |
| time(37)          | 不限  | 37              |
| rlp(39)           | UDP | 39              |
| nameserver(42)    | 不限  | 42              |
| ni cname (43)     | TCP | 43              |
| domain (53)       | 不限  | 53              |
| bootps(67)        | UDP | 67              |
| bootpe(68)        | UDP | 68              |
| tftp(69)          | UDP | 69              |
| 1 2 3 4 5 6 7 8 9 |     |                 |

可以通过输入协议名称和端口来进行已配置服务的查询。

点击"**添加**"



| <u>服务</u> 服务组 | 服务器地址 自定义网段     |
|---------------|-----------------|
| Service       |                 |
| Service名称     | smtp(25) *      |
| 协议            | TCP .           |
| 端口            | 25 0表示不限端口号 *   |
| 所属服务组         | ◎ 上邻居服务组 -> <-> |
| 注:右边有*号的项     | 目必须输入。          |
|               | 保存 圖除 取消        |

| 配置项:       | <u>说明</u>            |
|------------|----------------------|
| Service 名称 | 填入需要保护服务的名称或应用程序的名称。 |
| 协议         | 根据该服务使用的协议来选择。       |
| 端口         | 填写该服务调用的端口号。         |
| 所属服务组      | 如果定义了服务组,可将此服务添加到该服务 |
|            | 组。                   |

"服务组"的设置请参照"协议端口设定"-"服务组"

#### 服务组

服务组是服务的组合,比如用户可将上网所需服务加入至一个组

合,在配置"访问控制"策略时只需添加一个服务组即可。

点击"**服务组**",系统显示目前已经配置的服务组。



点击"**添加**"



| 服务 <u>服务组</u> 」 | 服务器地址 自定义网段  |        |
|-----------------|--|--------|
| 服务组             |  |        |
| 服务组名称           | 网上邻居服务组  | *      |
| 服务组描述           |  | A<br>7 |
| 服务              | echo(7)<br>discard(9)<br>systat(11)<br>daytime(13) | •      |
| 注:右边有*号的项目必须输   | ì入。  |        |
|                 | 保存 圖除 取消   |        |

| 配置项:  | <u>说明</u>                     |
|-------|-------------------------------|
| 服务组名称 | 自定义服务组的名称。                    |
| 服务组描述 | 对该服务组的详细说明,如应用场合、哪些应<br>用系统等。 |
| 服务    | 将此服务组需要用到的服务移到右边的方框<br>中。     |

### 服务器地址

定义网络中需要被访问的服务器。在访问控制策略中可以设置对此服务器访问控制。

点击"服务器地址"标签中的"添加"

| 服务 服务组    | 服务器地址  | 自定义网段 |           |
|-----------|--------|-------|-----------|
| 服务器地址     |        |       |           |
|           |        |       | <u>帮助</u> |
| 服务器名称     |        |       | *         |
| IP地址      |        |       | *         |
| 描述        |        |       | 4<br>7    |
| 注:右边有*号的项 | 目必须输入。 |       |           |
|           | 保存取消   |       |           |

| 配置项:  | <u>说明</u>        |
|-------|------------------|
| 服务器名称 | 填入可区别的服务器名称。     |
| IP 地址 | 填入该服务器准确的 IP 地址。 |



描述

填入该服务器的详细信息。

### 自定义网段

作为 IP 组的补充, 定义被访问的网段。

点击"自定义网段"标签的"添加"

| 服务 服务组                          | 服务器地址 <u>自定义网段</u> |
|---------------------------------|--------------------|
| <b>自定义网段</b><br><sub>网段名称</sub> | *                  |
| 开始IP地址                          | *                  |
| 结束IP地址                          | *                  |
| 描述                              |                    |
| 注:右边有*号的项目必须                    | 页输入。               |
|                                 | 保存取消               |

| 配置项:     | <u>说明</u>     |
|----------|---------------|
| 网段名称     | 填入有别于其他网段的名称。 |
| 开始 IP 地址 | 自定义网段的起始地址。   |
| 结束 IP 地址 | 自定义网段的结束地址。   |
| 描述       | 对网段的具体描述      |

# 7.3. 防护策略

# 7.3.1. 配置介绍

管理员在此集中配置防护策略,包括:访问控制策略、流量控制 策略、攻击防护策略和 ping 控制策略。

#### 访问控制

对客户端的连入连出网络访问进行控制,点击"**访问控制**",系 统显示预设的防火墙规则。



| 122 Mil 45 Mil                              | 28 S. (  | THE            | 操作类型                              | 0.9597.8 | MARKER |
|---|--|----------------|-----------------------------------|----------|--------|
| CAUXINEE THEFT                              |  | 建生             | 1013                              | 4        | -      |
| 2011年1月16日5月11日月月1日日日<br>1月11日日日<br>1月11日日日 |  | 18.21          | 会会试验完整补始行。不<br>成立时间出现学,然后不<br>除行  | ~        | *      |
| 朝止北方自法官の利止主要                                |  | 遗生             | 790                               | 4        |        |
| triessures.                                 |  | 12.25          | 6813                              | 1        | -      |
| STRUCTURE STRUCTURE                         | 相思知闻,安全部纪代器时才代许<br>第四语生。高明不允许是生,并非<br>不用户。提供上印的首个马成表着<br>重要的问题。  | ise:           | 常常的名词称"新闻",不<br>然后的第三届中,如何不<br>例行 | -        |        |
| esattan teriner (mar.)<br>Februari          | 特别的第一方面是因为我的计方语<br>的行为的这一种上帝的是比较多。<br>我们不会是这一种是不能产品。<br>我们在我们的是你们的不知道,<br>你不信意的问题。                                 | i <b>8:2</b> 1 | 来当时会常着时始行,不<br>成立时始出越来,然而不<br>例行  | -        |        |
| N & ROLLAND CHARACTER                       | · · · · · · · · · · · · · · · · · · ·  | 18.21          | 会社の完美社会行、7<br>第二世的記述者で、第二世<br>第17 | -        |        |
| THE TREME OF STREET                         | 代置制度。九年间一子印度制度基础<br>11月上市制造成工具、数字为一面<br>"基本体制度基础。例上市制造的<br>发现。实际的生成基础。一面标题在的<br>度计划上的影响和这种,可能能能<br>同时的中级生成和成本与的实现。 | ал.            | 940                               | -        |        |
| NUMBER OF STREET                            | 村田和田、田山田和田和田村上<br>市市市市工作、西山市一市"市市<br>市、市市市市市市市市市市市<br>市村工作市市市市市市市市市市<br>市村工作市市市市市市市市市市                             | ал.            | 700                               | -        |        |
| MINIMUSACES.                                | HENRI - MILHARADOSE<br>A. SERIADOSE 8. ANT<br>SERIADOSE 8. ANT   | άλ             | 不能性                               | *        | ~      |

点击"**添加"**按钮,进入添加"访问控制策略"。





| 配置项: | <u>说明</u>  |  |  |
|------|--|--|--|
| 策略名称 | 填入策略名称。  |  |  |
| 策略描述 | 填入策略的详细描述。   |  |  |
| 方向   | 设定此策略控制的访问方向   |  |  |
| 远端网段 | 本系统无需设置本端地址,本地地址总是客户端自身的 IP 地址。远端网段可以按以下 3 种方式设置。<br>1、不限:远端地址为任意地址<br>2、同一子网-子网掩码数:如果填入相应的掩码数,则根据掩码数计算子网地址<br>3、以下网段或服务器:选择相应的目标网段或服务器。   |  |  |
| 服务   | 选择此策略需要控制的服务。  |  |  |
| 服务组  | 选择此策略需要控制的服务组。   |  |  |
| 操作类型 | <ul> <li>共有 5 种类型:</li> <li>1、放行。对匹配本条策略的网络访问放行,对用户没有任何提示。</li> <li>2、不放行。对匹配本条策略的网络访问不放行,对用户没有任何提示。</li> <li>3、安全基线完整时放行。对于匹配本条策略的网络访问,如果客户端的安全基线合格就放行,不合格不放行,对用户没有任何提示。</li> <li>4、安全基线完整时放行,不满足时给出提示,然后放行。对于匹配本条策略的网络访问,无论客户端的安全基线是否合格,都放行,但对安全基线不合格的电脑弹出提示窗口。</li> <li>5、安全基线完整时放行,不满足时给出提示,然后不放行。对于匹配本条策略的网络访问,如果客</li> </ul> |  |  |

|        | 户端的安全基线合格就放行,不合格不放行,并<br>对安全基线不合格的电脑弹出提示窗口。  |
|--------|--|
| 访问进程   | 填入需要匹配的进程名称,不包含完整路径,多个进程用'/'隔开,也可从己定义的白名单中获取。若不填,则不对进程进行匹配。  |
| 记入日志方式 | 连接日志记录在客户端防火墙日志里面,可以根据需<br>要选择何种方式记入日志。主要有以下几种方式:"不<br>记入日志"、"被策略允许时记入日志"、"被策略<br>拒绝时记入日志"、"总是记入日志"。 |
| 拒绝访问时的 | 当防火墙拦截客户端的数据访问时,给出特别的提   |
| 个性化信息  | 示,可自定义。  |
| 在线模式   | 配置在线和离线时是否生效   |
| 策略应用对象 | 将此策略应用到 IP 组,工作组,主机名或用户组   |
| 所属分组   | 在策略浏览时能够按照分组显示。<br>系统安装时自动创建一个名为"默认分组"的组名。<br>或可以自行创建分组,名称另行定义                                       |

**注意**:多条访问控制策略应用到同一个 IP 组或用户组时,这些策略的匹配是分先后顺序的,可通过上下箭头来调整顺序,类似路由 ACL。

#### 流量控制

流量控制规则精细控制每个用户电脑中的每个进程访问网络中 不同的网段和主机时所能占用的带宽。良好的流量控制规则能在 蠕虫病毒爆发时自动遏制其占用的网络带宽,始终保持网络通 畅。

点击"**添加**"



| 数 收击防护 PING控制  |
|--|
|  |
| ·  |
| *  |
| * 按远端端口统计  |
| 不時 •   |
| 四/2 💌 🗆 不限制带宽 🗆 不记入总读量                                     |
| - 墨个网络-  |
| •  |
| 不记入日志  |
| <ul> <li>● 新育时間 ○ 1作时間 ○ 第1作时間 ○ 以下时間段</li> <li></li></ul> |
| 图 在纸时生效 图 扁纬时生效  |
| (还没有应用到任何对象) 型盘及振机   |
| 全時   |
| jing   |
| 浅稿入。<br>  <u>御神</u>   [ <b>雅</b> ] [ <b>雅</b> ] [ ]        |
| <u>说明</u>  |
| 填入流量策略的名称。   |
| 共有3种控制类型:按远端端口,按本端端口,                                      |
| 按进程。   |
|  |
| 选择远端端口的协议类型  |
| 填入允许的最大流量值,单位是 KB/S 或%。KB/S                                |
| 表示采用带宽绝对值,%表示使用网卡带宽的百                                      |
| 分比。  |
| 不限制带宽表示对此类流量不进行管理和控  |
| 制。   |
| 不记入总流量,如果在" <b>基本配置</b> "里设定了                              |
| 客户端总带宽,而在此设置" <b>不记入总流量</b> ",                             |
| 则此类流量不统计在总流量中,即此类流量只                                       |
|  |



|          | 受此处设置的影响,而不受终端总带宽的影响。         |
|----------|-------------------------------|
|          | 填入远端 IP 的起始和结束地址,若地址不限请       |
| 远端 IP 范围 | 点击" <b>整个网络"</b> 。开始和结束地址都为0表 |
|          | 示整个网络。                        |
| 描述       | 填入此规则的详细描述。                   |
| 远端端口     | 填入需要控制的远端端口号。                 |
| 按本地端口统计  |                               |
| 协议       | 选择本地端口的协议类型                   |
|          | 填入允许的最大流量值,单位是 KB/S 或%。KB/S   |
|          | 表示采用带宽绝对值,%表示使用网卡带宽的百         |
|          | 分比。                           |
|          | 不限制带宽表示对此类流量不进行管理和控           |
| 带宽       | 制。                            |
|          | 不记入总流量,如果在"基本配置"里设定了          |
|          | 客户端总带宽,而在此设置"不记入总流量",         |
|          | 则此类流量不统计在总流量中,即此类流量只          |
|          | 受此处设置的影响,而不受终端总带宽的影响。         |
|          | 填入远端 IP 的起始和结束地址,若地址不限请       |
| 远端 IP 范围 | 点击" <b>整个网络</b> "。开始和结束地址都为0表 |
|          | 示整个网络。                        |
| 描述       | 填入此规则的详细描述。                   |
| 本地端口     | 填入需要控制的本地端口号                  |
| 按应用程序统计  |                               |
| 协议       | 选择本地端口的协议类型                   |
| ill an   | 填入允许的最大流量值,单位是 KB/S 或%。KB/S   |
| 带蒐       | 表示采用带宽绝对值,%表示使用网卡带宽的百         |



|                              | 分比。                           |  |  |  |
|------------------------------|-------------------------------|--|--|--|
|                              | 不限制带宽表示对此类流量不进行管理和控           |  |  |  |
|                              | 制。                            |  |  |  |
|                              | 不记入总流量,如果在" <b>基本配置</b> "里设定了 |  |  |  |
|                              | 客户端总带宽,而在此设置"不记入总流量",         |  |  |  |
|                              | 则此类流量不统计在总流量中,即此类流量只          |  |  |  |
|                              | 受此处设置的影响,而不受终端总带宽的影响。         |  |  |  |
|                              | 填入远端 IP 的起始和结束地址,若地址不限请       |  |  |  |
| 远端 IP 范围                     | 点击" <b>整个网络</b> "。开始和结束地址都为0表 |  |  |  |
|                              | 示整个网络。                        |  |  |  |
| 描述                           | 填入此规则的详细描述。                   |  |  |  |
|                              | 填入需要控制流量的进程名,不包含完整路径,         |  |  |  |
| 进程名                          | 多个进程用"/"隔开。也可点击" <b>获取白名单</b> |  |  |  |
|                              | 进程"从白名单列表中添加进程。               |  |  |  |
|                              | 主要有两种方式: "不记入日志"和"总是记         |  |  |  |
| 记入日志方式                       | 入日志"。生成的日志记录在客户端防火墙日          |  |  |  |
|                              | 志里面。                          |  |  |  |
| 在线模式                         | 配置在线和离线时是否生效                  |  |  |  |
| <b>举</b> 政 应田 <del>动</del> 色 | 将此策略应用到 IP 组,工作组,主机名或用户       |  |  |  |
| 來咱应用刈爹                       | 组                             |  |  |  |

### 攻击防护

攻击防护阻止终端发送欺骗包或攻击包以及未知的流量攻击包,确保内网正常运行。在此可添加防 ARP 欺骗、防 IP 仿冒等功能。 点击"添加"



| 动间腔时 波   |                   | PING 2        | <u> </u>    |                 |
|--|-------------------|---------------|-------------|-----------------|
| 攻击防护   |                   |               |             |                 |
| 解點 主称<br>四州 wat 均衡的 #5<br>点叫 wat 法求 我都当他答<br>四明 55 H H K 自己的算法 |                   | tert          |             |                 |
|  |                   | 同时处理实研        | 和描述的APP IS  | •               |
|  |                   | 0.8-0 Z       |             | _ 1004          |
|  |                   | *#0Z          |             |                 |
| 原始推荐建设访问   | 86                | * # C Z       |             |                 |
| 过渡时伪留数据包   |                   | ****          |             |                 |
| 107相关 @表示不   | 890               |               |             |                 |
| 每进程对外和中共发  | 连接就限制             | 高都構造10        | (新参加設備 0    |                 |
| 都进程每秒过外TCF   | 并发达抽炸限制           | 合物简直 10       | 「秋水」院道(0    |                 |
| 元TCF跟参加当进程   |                   |               |             | (金加 <i>港 程</i>  |
|  |                   | -             |             | <b>期</b> 教室通程   |
| mr相关的表示不同  | RMD               |               | -           |                 |
| 每进程每秒发送(0)*  |                   | 高智術値 10       | 印刷机器值包      |                 |
| <b>动法权局约</b> 五式(1)   | ELEFT FRALES      | 合物素值 10       | 印書開建 印      |                 |
| <b>希好发展印度</b> 目的   |                   | 古物间值 10       | 同意調査 0      |                 |
| 0035489 834 080  |                   | 60            |             | 0表示使用數以时间间至60%) |
| 无印刷制的进程  |                   | -             |             | State and Ann   |
|  |                   |               |             | (1000 at 42     |
| 记入日本有望   | 7010              |               |             |                 |
| 生效时间   | - TEADS           | O TANK D a    | TABLE       | T0+1015         |
| · · · · · · · · · · · · · · · · · · ·                          |                   | 1016          | 11FEIH 00   |                 |
|  | 2012-02-          | 10.9:00       | 2012-02-10  | 13:30           |
|  |                   | Alex Alex     | 1           | H. H. H.        |
| 在线模式   | 团在线时生             | 效同高线时生效       |             |                 |
| 擁職应用対象   | (还没有应用            | 到任何对象) 正      | 后沿線鐵        |                 |
| 0.08 = 10  |                   |               |             |                 |
| (1146-1142   | ±49               |               |             |                 |
| 创建者  | ting              |               |             |                 |
| 注:名边有+号的项目   | 日台清新入。<br>【保存】 取消 |               |             |                 |
| 配置项:   | <u>说明</u>         |               |             |                 |
| 至  | <br>              | 攻击防护行         | 等略称         |                 |
| < ►µ ^µ /小<br>   |                   |               | יניין ⊔⊶∽וי |                 |
|  | 共有                | 4个选项 <b>:</b> |             |                 |
|  | 1,                | 不启用。          |             |                 |

| 2、 | 过滤 | 发送的  | ARP 包。 | 对发达 | 送的 AR | P包进 | 行检  |
|----|----|------|--------|-----|-------|-----|-----|
|    | 查, | 如果发现 | 见欺骗往   | 亍为, | 则 ARP | 包被表 | ら弃。 |

| 启用 ARP 欺骗防护 | 0  |                            |
|-------------|----|----------------------------|
|             | 3, | 过滤的 ARP 包。 对接收的 ARP 包进行检查, |
|             |    | 如果发现欺骗行为,则 ARP 包被丢弃。       |
|             | 4  |                            |

|                             | ARP 包被丢弃。   |
|-----------------------------|---|
| 启用 ARP 请求超时<br>拒答           | 若选择启用,客户端发送 ARP 请求后如果 5 秒<br>内没有应答包,后面的收到的应答包将被丢弃。  |
| 启用网关 MAC 自动<br>绑定           | 若选择启用,客户端在线状态下自动绑定当前<br>网关的 MAC 地址,而对从网络上接收到的关于<br>网关的 ARP 包不进行处理。客户端在离线状态<br>下自动解除绑定。          |
| 限制隐藏进程网<br>络访问              | 若选择启用,则拦截隐藏进程的网络访问。有些木马程序在 Windows 任务管理器中是看不到的。此选项只有在"访问控制"的日志选项为<br>"记入日志"时才有效。                |
| 过滤 IP 仿冒数据<br>包             | 客户端发包时如果 IP 包的源 IP 地址与自身的<br>IP 地址不相符,则被认为是 IP 仿冒行为。若选<br>择启用,系统将拦截仿冒的 IP 包。                    |
| TCP 相关                      | 设定阈值限制客户端的 TCP 连接行为。在 TCP<br>相关的设置中,如果数值为 0,则表示对该项目<br>不限制。                                     |
| <i>每进程对外</i> TCP<br>并发连接数限制 | 系统对每个进程的 TCP 连接进行监控和统计,<br>当一个进程的并发连接数(保持的连接数)超<br>过设定的阈值后,将被限制或告警。建议根据<br>网络的实际情况进行调整、优化。      |
| 每进程每秒对外<br>ICP 并发连接数限<br>制  | 系统对每个进程的 TCP 连接进行监控和统计,<br>当一个进程的每秒并发连接数(每秒新发起的<br>连接数)超过设定的阈值后,将被限制或告警。<br>建议根据网络的实际情况进行调整、优化。 |
| 无 TCP 限制的进程                 | 设置无 TCP 连接数限制的进程,如某些业务进程。   |



| UDP 相关                       | 设定阈值限制客户端的 UDP 发包行为。在 UDP<br>相关的设置中,如果数值为 0,则表示对该项目<br>不限制。  |
|------------------------------|--|
| <i>每进程每秒发送<br/>UDP 包数</i>    | 系统对每个进程的 UDP 连接进行监控和统计,<br>当一个进程的每秒 UDP 发包数超过设定的阈值<br>后,将被限制或告警。建议根据网络的实际情<br>况进行调整、优化。                            |
| <i>每进程每秒发送</i><br>UDP 包目标地址数 | 系统对每个进程的 UDP 连接进行监控和统计,<br>当一个进程的每秒发送 UDP 包的目标地址数超<br>过设定的阈值后,将被限制或告警。建议根据<br>网络的实际情况进行调整、优化。                      |
| <i>每秒发送 UDP 包<br/>总数</i>     | 当客户端所有进程发送 UDP 包数超出阈值时,<br>将被限制或告警。建议根据网络的实际情况进<br>行调整、优化。   |
| UDP 限制时长(秒)                  | 当 UDP 发包行为超出限制阈值时,系统将对该<br>进程继续发包禁止一段时间,在这里设置这个<br>禁止发包的时间长度。如果是"每秒发送 UDP<br>包总数"超过限制阈值,则任何进程的 UDP 的<br>发包行为都会被禁止。 |
| 无 UDP 限制的进程                  | 设置无 UDP 发送数限制的进程,如某些业务进程。  |
| 记入日志方式                       | 主要有两种方式: "不记入日志"和"总是记入日志"。生产的日志记录在客户端防火墙日志里面。  |
| 在线模式                         | 配置在线和离线时是否生效   |
| 策略应用对象                       | 将此策略应用到 IP 组,工作组,主机名或用户<br>组   |

198



**注意**: 当达到告警阀值时,天珣客户端图标将变黄,发出告警,同时在客户端日志中可查看到告警日志。

### PING 控制

Ping 控制指的是对客户端的 ICMP 协议进行控制,可控制其 ping 出或者是被 ping。

点击"**添加**"

| PING控制  |                            |            |                 |
|---------|----------------------------|------------|-----------------|
| 策略名称    |                            |            |                 |
| 제略표년    |                            | (a)        |                 |
| 允许PING出 |                            | *          |                 |
| 允许被PING | ***0A<br>**0a              |            |                 |
| 记入日志方式  | 不记入日志                      |            |                 |
| 生效时间    | ● 所有时间 ◎ 工作时间 ◎ 非工作时间      | 0 以下时间成    |                 |
|         | [1012-03-10 0:00 ] [2013-0 | 5-10-13:30 | -1419<br>  E.M. |
| 在纸模式    | 图 在线时生效 图 高线时生效            |            |                 |
| 解释应用对象  | (进没有应用到任何对象) <u>重叠是课稿</u>  |            |                 |
| 创建类型    | 全局                         |            |                 |
| -       | 1100                       |            |                 |

| 配置项:      | <u>说明</u>                 |
|-----------|---------------------------|
| 策略名称      | 填入策略名称。                   |
| 策略描述      | 填入策略的详细描述。                |
| 允许 PING 出 | 设定是否允许 PING 出             |
| 允许被 PING  | 设定是否允许被 PING              |
| 记入日志方式    | 主要有两种方式:"不记入日志"和"总是记入日志"。 |
|           | 生成的日志记录在客户端防火墙日志里面。       |
| 在线模式      | 配置在线和离线时是否生效              |



**策略应用对象** 将此策略应用到 IP 组,工作组,主机名或用户组

## 7.3.2. 配置要点

- 点击"访问控制"中的"添加"按钮,输入策略名称为"安 全基线不满足,http访问提示并不放行!"
- 2. "方向"选择为"连出"
- 3. "远端网段"选择"不限"
- 点击"服务"的"编辑"按钮,进入后选择"http(80)协议
   TCP 端口 80"
- "操作类型"选择"安全基线完整时放行,不完整时给出提示,然后不放行"
- 6. "记入日志方式"选择"被策略拒绝时记入日志"
- 7. "在线模式"选择"在线时生效"
- 点击"策略应用对象"的"查看及编辑"按钮,选择应用对 象类型及终端,"确定"然后"保存"
- 9. 点击"流量控制"中的"添加"按钮,输入策略名称为"限制 HTTP 带宽"
- 10. "控制类型"为"按远端端口统计",协议为"不限"
- 11. "带宽"设置为 50KB/S, 远端 IP 范围选择"整个网络"
- 12. "远端端口"设为80
- 13. 选择"在线时生效",并点击"策略应用对象"的"查看及编辑"按钮,选择应用对象类型及终端,"确定"然后"保存"
- 14. 点击"**攻击防护**"中的"添加"按钮,输入"策略名称"为 "攻击防护策略"
- 15. "启用 ARP 欺骗防护"选择"同时处理发送和接收的 ARP 包"
- 16. "启用网关 MAC 自动绑定"选择"是","过滤 IP 仿冒数据包"选择"是"



- 17. "每进程对外 TCP 并发连接数限制"中的"告警阀值"设为70, "限制阀值"为100
- 18. "每进程每秒对外 TCP 并发连接数限制"中的"告警阀值"设为 70, "限制阀值"为 100
- 19. 选择"在线时生效",点击"策略应用对象"的"查看及编辑"按钮,选择应用对象类型及终端,"确定"然后"保存"
- 20. 策略配置好后,属于"防火墙组"的终端在安全基线不满足 要求的情况下,会被禁止进行 80 端口的访问,而即使能进 行 80 端口访问,最大带宽也只有 50KB/S,最大限度限制了 终端进行上网操作时所占用的带宽。另外启用了 ARP 欺骗防 护,并限制了 TCP 的发包数,可以防止客户端发生 ARP 攻击 或被攻击。

# 7.4. 访客策略

### 7.4.1. 配置介绍

网络准入中对于外来的安装了客户端的电脑,其只能使用匿名登录,那么可以获取访客策略。此策略一般定义为权限最小的访问策略。

#### 访问控制

对于匿名登录的用户,可以用访问控制规则来限制访客的网络访问行为。一般在此只设置最必要的允许规则,最后以拒绝规则结束。

点击"**添加**"



| 访问控制-访客                             | 策略                  |                        |          |
|-------------------------------------|---------------------|------------------------|----------|
|                                     |                     |                        |          |
| 兼職名称                                |                     |                        |          |
| 蒲畦描述                                |                     | 14                     |          |
|                                     |                     |                        |          |
| 协议                                  | 不跟                  |                        |          |
| <b>14</b> 0                         |                     |                        |          |
| Consider the address and the second |                     |                        |          |
| 2794024217-904L                     |                     |                        |          |
| 运输结束证用址                             |                     |                        |          |
| 操作类型                                | +++++选择操作类型+++++    |                        |          |
| 记入日志方式                              | 不记入日志               |                        |          |
| 生效时间                                |                     | тана 🔿 и тнас          |          |
|                                     | AMUA                | 11.2.1.1.1<br>11.2.1.1 |          |
|                                     | 2012-02-10-9:00     | 2010-00-10 15:30       | - 5 (10) |
| 在绒蠟式                                | III 在城时生效 III 高级时生效 |                        |          |
| 解释应用对象                              | (还没有应用到任何对象) 型質     | 基编辑                    |          |
| 的建共型                                | 2 <b>M</b>          |                        |          |
| 创建表                                 | jing                |                        |          |

| 配置项:       | <u>说明</u>                    |
|------------|------------------------------|
| 策略名称       | 填入有别于其他访问控制规则名称。             |
| 策略描述       | 填入该规则的详细信息。                  |
| 协议         | 选择访问控制的协议。                   |
| 端口         | 访问远程机器的端口号。                  |
| 远端起始 IP 地址 | 填入准确的 IP 地址                  |
| 远端结束 IP 地址 | 填入准确的 IP 地址                  |
| 操作类型       | 选择是否放行以上定义的网络访问              |
| 记入日志方式     | 选是否记入日志。                     |
| 在线模式       | 配置在线和离线时是否生效                 |
| 策略应用对象     | 将此策略应用到 IP 组,工作组,主机名或用户<br>组 |

### 流量控制



对于匿名登录的用户,设置专门的访客流量控制规则,以防止因 为它的异常运行而对网络有显著的影响。

| 点击 <b>"你加</b> ) |
|-----------------|
|-----------------|

| 访问控制 查里控制       |                                       |
|-----------------|---------------------------------------|
| 流量控制-访客策略       | ¥                                     |
| 策略名称            |                                       |
| 開業構建            | *                                     |
| 控制类型            | → 按远端端口统计                             |
| 15 R            | 不開 -                                  |
| 带宽              | 129/2 💽 🗇 不解刺帶変 🗇 不记入息发量 •            |
| 过程中范围           | - 華小同雄)-                              |
| 远搁端口            |                                       |
| 记入日志方式          | · · · · · · · · · · · · · · · · · · · |
| 生效时间            | ● 新有时间 ○ 工作时间 ○ 非工作时间 ○ 以下时间很         |
|                 | 开始时间 悠史时间 唱儀 網絡                       |
| 8               | 3012-03-10 9200                       |
| 在线模式            | 图 在线时生效 图 高线时生效                       |
| 策略应用对像          | 《还没有应用到任何对象》 宣誓及道道                    |
| 创建类型            | <b>主助</b>                             |
| 討連典             | ing                                   |
| 注:右边角×号的谈目必须    | 前入。<br>保存 取消                          |
| 配置项:            | <u>说明</u>                             |
| 策略名称            | 填入有别于其他流量控制的策略名称。                     |
| 1.2. 16.1 MA TH | 共有两种控制类型:按远端端口控制和按本端                  |
| 控制类型            | 端口控制                                  |
| 按远端端口统计         |                                       |

| 协议 | 选择远端端口的协议类型                 |
|----|-----------------------------|
|    | 填入允许的最大流量值,单位是 KB/S 或%。KB/S |
|    | 表示采用带宽绝对值,%表示使用网卡带宽的百       |
| 带宽 | 分比。                         |
|    | 不限制带宽表示对此类流量不进行管理和控         |
|    | 制。                          |



|          | 不记入总流量,如果在"通用控制"里设定了                            |
|----------|---|
|          | 客户端总带宽,而在此设置"不记入总流量",                           |
|          | 则此类流量不统计在总流量中,即此类流量只                            |
|          | 受此处设置的影响,而不受终端总带宽的影响。                           |
| 远端 IP 范围 | 填入远端 IP 的起始和结束地址,若地址不限请                         |
|          | 点击"整个网络"。开始和结束地址都为0表                            |
|          | 示整个网络。  |
| 描述       | 填入此规则的详细描述。                                     |
| 远端端口     | 填入需要控制的远端端口号。                                   |
| 创建状态     | 全局管理员创建的规则,创建状态为全局。本                            |
|          | 地管理员创建的规则, 创建状态为本地。                             |
| 创建者      | 创建者管理员的名称                                       |
| 按本地端口统计  |   |
| 协议       | 选择本地端口的类型                                       |
| 带宽       | 填入允许的最大流量值,单位是 KB/S 或%。KB/S                     |
|          | 表示采用带宽绝对值,%表示使用网卡带宽的百                           |
|          | 分比。   |
|          | 不限制带宽表示对此类流量不进行管理和控                             |
|          | 制。  |
|          | 不记入总流量,如果在"通用控制"里设定了                            |
|          | 客户端总带宽,而在此设置"不记入总流量",                           |
|          | 则此类流量不统计在总流量中,即此类流量只                            |
|          | 受此处设置的影响,而不受终端总带宽的影响。                           |
|          |   |
|          | 填入远端 IP 的起始和结束地址,若地址不限请                         |
| 远端 IP 范围 | 填入远端 IP 的起始和结束地址,若地址不限请<br>点击"整个网络"。开始和结束地址都为0表 |



| 本地端口   | 填入需要控制的本地端口号                 |
|--------|------------------------------|
| 在线模式   | 配置在线和离线时是否生效                 |
| 策略应用对象 | 将此策略应用到 IP 组,工作组,主机名或用户<br>组 |

注意:访客策略只对网络准入时使用"匿名登录"的终端生效。

# 8.补丁管理

# 8.1. 关于补丁管理

天珣"补丁管理":是由天珣策略服务器提供的补丁管理方案,可以通过"在线补丁源"或"WSUS补丁源"为各终端补丁修复。 三种补丁源及补丁发布安装示意图



- 天珣补丁管理分三种补丁源:在线补丁源、WSUS 补丁源和
   手工补丁源。
- 内网部署离线补丁是在线补丁源的一种发布模式,请参考
   《配置手册-离线补丁》
- 配置完补丁源并发布后,如果不使用本系统的强制安装补丁 功能,请到"补丁管理"→"补丁分发"中进行补丁分发其 他项目的配置和操作。
- 如果您要使用强制补丁功能,请到"安全基线"→"补丁强



制策略"中进行配置和操作。

天珣补丁管理系统维护的 Windows 版本包括:英文版、简 体中文版和繁体中文版的操作系统。

#### 名词解释

- "在线补丁源":由天珣研发团队测试维护的补丁库,补丁 源地址为:<u>http://patch.patchsource.cn</u>,其中的补丁文件来 自微软官方网站,并已经经过了天珣研发团队的测试。
- "WSUS"集成管理:天珣客户端可代替 WSUS 客户端实现 WSUS 内网补丁分发。
- "手工补丁源":可由管理员自行从微软网站下载、测试并发 布到天珣"手工补丁源","手工补丁源"补丁发布模式和"在 线补丁源"发布模式相同。

# 8.2. 在线补丁源

### 8.2.1. 关于在线补丁源

- "在线补丁源"按同步方式分"互联网同步"和"离线同步"
   两种方式。
- "在线补丁源"可以和 WSUS 集成管理同时使用。
- "在线补丁源"维护了 Windows 系统安全补丁、IE Explorer 安全更新补丁、Outlook 安全更新补丁。
- 涉及到正版验证的补丁并未发布,正版验证补丁需要用户单独 确认授权许可并确认更新。
- ■补丁分发默认会自动分发,支持分发前对补丁进行测试。

**重点:**在线补丁是由天珣补丁精灵实现补丁分发,因此支持非系统管理员自动安装补丁,支持 AD 域环境的补丁更新。


#### 名词解释

"补丁列表":在线补丁源获取的补丁信息和手工补丁创建的补丁 信息,都包含在此列表中。列表中的补丁必须经过发布才能通过补 丁管理功能向客户端分发。

**"系统设置"**:系统供应商在互联网上设置在线补丁源,为用户提供 Windows 操作系统安全补丁下载更新。本系统在此处配置与在线补丁源连接的相关参数,包括同步服务 URL、用户许可信息、服务参数等。

"系统控制":补丁同步服务的控制面板,通过 WEB 与补丁同步 服务通讯,执行补丁同步、查询同步状况等任务。

"同步日志":查看补丁同步服务器的运行日志,若补丁同步任务 出现问题可在此查看相关日志。

"同步状态":查看各个补丁同步服务器同步补丁文件的状态。其 中查询中心服务器显示的是从互联网上在线补丁源同步补丁的状态,查询各个本地服务器显示的是本地服务器从中心服务器同步补 丁的状态。

### 8.2.2. 配置介绍

| <b>ト丁列</b> 3 | ŧ.  |  |          |     |              |
|--------------|-----|--|----------|-----|--------------|
| <b>**</b>    | T4  | 3  |          |     |              |
| 20           | 2.8 | Eif .  | 19+21    | 45W | <b>E</b> 365 |
| 1303052      | 35  | Tindows 影响网络联展系(IDE)的最近可能会允许执行程序代码             | 1004-008 | 22  | 4            |
| DE15710      | 兼統  | 書寫波 Gasser)符丁                                  | 110-1011 | PE  | 4            |
| 1002301      | 王统  | Naroseft Jet营业库引擎中的漏洞可能导致代码推执行                 | 1004-014 | 82  | 4            |
| 13042074     | 系统  | 權和和文持中心中的交生黨調可能会允许這種共行代码                       | 1504-015 | 22  | 4            |
| 13042528     | 355 | 工具管理器中的高限可能允许执行代码                              | #204-019 | 22  | *            |
| CR4:172      | 系统  | 任务计划程序中的编词可能允许执行代码                             | 100-002  | 严重  | 4            |
| 12041015     | 系统  | 和此、帮助中的影响可能化冲铁符代码                              | M004-023 | 78  | 4            |
| 00066        | 系统  | Tindows Shell 中的病洞可能化许该提供信代码                   | #504-024 | 22  | 4            |
| DECUSE       | 35  | TelOW 28. Records Xuolice 中的公告伝题漏洞可能导致"拒绝影乐"功击 | M204-030 | 22  | .#           |
| B84(53)      | 兼統  | Nation 中的展开可能允许执行这些代码                          | #304-031 | 82  | A            |
| 12235        |     | 10   |          |     |              |

补丁列表页面



|       | 按补丁名称查询某个补丁是否已经  |
|-------|------------------|
| 按补丁名  | 存在于天珣的补丁列表中,如查询  |
|       | KB958644         |
|       | 按补丁的安全公告查询某个补丁是  |
| 按安全公告 | 否已经存在于天珣的补丁列表中,如 |
|       | 查询 MS04-031      |

### 系统设置页面

in the

| 系统设置                     |                                    | 应用新贺 | <u>ME</u> |
|--------------------------|------------------------------------|------|-----------|
| <b>医外颈结</b> 肌            |                                    |      |           |
| <b>股2官师</b>              | <b>能增加</b>                         |      |           |
| 同步服务101.                 | http://putch.patchnowce.cn         |      | 1         |
| 补丁文件下载模mu.               | http://192.168.1.15.9833/Nownland/ |      | 1         |
| 补丁文件下截相对332.             | AutoOpdate/                        |      | 1         |
| 周步文件到目录(加不使用数以配置,输入绝对路径) | Devalord Autolydate                |      | 2         |

| 配置项:  | <u>说明</u>  |  |  |
|---|--|--|--|
| 应用配置  | 系统下载服务配置项立即重新加载的选<br>项。  |  |  |
| 系统供应商在互联网上设立的在线补口         同步服务 URL       源 的 网 址 , 默 认 プ <u>http://patch.patchsource.cn</u> 。 |  |  |  |
| 补丁文件下载根 URL   | 下载根 URL与补丁文件下载相对 URL 共同组成中心服务器向本地服务器分发补丁文件的完整URL,其指向默认为中心服务器的下载虚拟目录。                           |  |  |
| 补丁文件下载相对<br>URL   | 与补丁文件下载根 URL 共同组成中心服务器向本地服务器分发补丁的完整 URL。<br>其指向一般为中心服务器下载虚拟目录<br>中存放补丁文件的子目录,例如<br>AutoUpdate。 |  |  |
| 同步文件到目录 (如不   | 填写中心服务器从在线补丁源下载补丁  |  |  |



| 使用默认配置, 输入绝 | 的存放路径,默认存放于中心服务器安            |
|-------------|------------------------------|
| 对路径)        | 装目录的 Download 目录下的           |
|             | AutoUpdate 目录中。可参考如下格式:      |
|             | Download\AutoUpdate\。如果不使用默认 |
|             | 配置,可输入存放补丁的绝对路径。请            |
|             | 注意,当不使用默认配置时,请确保在            |
|             | IIS 设置中,中心服务器下载虚拟目录所         |
|             | 指向的路径与此处输入的绝对路径一             |
|             | 致。                           |

| <b>服</b> 务参数            |            |   |
|-------------------------|------------|---|
| 620 W                   | <b>防衛協</b> |   |
| 每天启动两步时间 (KANA)         | 2300       | 1 |
| 信息同步起时时间(分钟)            | 30         | , |
| 文件同步超时时间(分钟)            | 300        | 1 |
| 间步文件到所有本地同步服务器战时时间(6)种) | 300        | 1 |

| 配置项:           | <u>说明</u>   |
|----------------|---|
| 每天启动同步时间(HHMM) | 设置中心服务器每天启动从在线补丁<br>源获取补丁更新的时间。系统默认值<br>为"2300",即中心服务器每天晚上23<br>时自动从在线补丁源获取更新文件。                                      |
| 信息同步超时时间(分钟)   | 设置中心服务器从在线补丁源获取补<br>丁更新信息(主要是补丁配置信息等)<br>的超时时间。系统默认值为"30",即<br>启动同步任务后 30 分钟仍无法获取到<br>补丁更新信息,则表示本次补丁配置<br>信息同步任务超时失败。 |
| 文件同步超时时间(分钟)   | 设置中心服务器从在线补丁源下载补<br>丁文件的超时时间。系统默认值为<br>"300",即启动同步任务后 300 分钟<br>仍无法完成补丁文件的下载,则表示                                      |



|                            | 本次补丁文件同步任务超时失败。                               |
|----------------------------|---|
| 同步文件到所有本地同步服<br>务器超时时间(分钟) | 设置本地服务器从中心服务器下载补<br>丁文件的超时时间。系统默认值为<br>"300"。 |

| 100.50 | 135.44 | 20 61  |
|--------|--------|--------|
| 10011  | 通為     | 101.40 |

| 配置導         | K20 |   |
|-------------|-----|---|
| 管理员接收通知邮件地址 |     | 1 |
| 发送邮件服务器     |     | , |
| 发话邮件用户名     |     | 1 |
| 发透廊件密码      |     | 1 |

| 配置项:        | 说明  |
|-------------|---|
| 管理员接收通知邮件地址 | 填写系统管理员接收通知邮件的地<br>址。配置好后,系统会向该地址发送<br>从在线补丁源更新补丁的情况报告。 |
| 发送邮件服务器     | 填写发送补丁更新报告邮件服务器的 IP 或 URL。系统可通过该邮件服务器,发送报告邮件。           |
| 发送邮件用户名     | 填写用于发送报告邮件的 Email 地址。                                   |
| 发送邮件密码      | 填写发送报告邮件的 Email 密码。                                     |

| 代理顧多諧波畫                |     |   |
|------------------------|-----|---|
| 新資源                    | 新聞協 |   |
| 使用http:代理服务器选闭Internet | đ   |   |
| 8777代理服务器线址            |     | 1 |
| x177代理服务图调口            |     | 1 |
| 町17代理芸会員は同用戸名          |     | 1 |
| XTTF代理服务器访问密码          |     | , |
| xTTP代理解务器以证赋           |     | 1 |

| 配置项:                        | 说明  |
|-----------------------------|---|
| 使用 HTTP 代理服务器访问<br>Internet | 在使用 HTTP 代理服务器上网的网络环境中,中心服务器需要通过<br>HTTP 代理服务器访问互联网上的在<br>线补丁源,此选项设置为"是"。 |
| HTTP 代理服务器地址                | 填写 HTTP 代理服务器的 IP 地址。   |
| HTTP 代理服务器端口                | 填写 HTTP 代理服务器的端口。   |
| HTTP 代理服务器访问用户名             | 设置通过 HTTP 代理服务器访问互<br>联网的用户名。   |
| HTTP 代理服务器访问密码              | 设置通过 HTTP 代理服务器访问互  |



|               | 联网的用户密码。                        |
|---------------|---------------------------------|
| HTTP 代理服务器认证域 | 设置通过 HTTP 代理服务器访问互<br>联网所需要的域名。 |

### 系统控制页面

| 系统设置 系统控制      | 同步日志 | 同步状态 |           |
|----------------|------|------|-----------|
| 系统控制           |      |      | <u>帮助</u> |
| 启动同步任务         |      |      | 开始        |
| 查询同步任务状况       |      |      | 开始        |
| 查看已连接的本地同步服务器  |      |      | 开始        |
| <b>清空补</b> 丁记录 |      |      | 开始        |
|                |      |      |           |

| 配置项:          | 说明   |
|---------------|--|
| 启动同步任务        | 系统默认每天 23 时自动启动从在线<br>补丁源同步补丁的任务,管理员也可<br>通过此按钮手工启动补丁同步任务。 |
| 查询同步任务状况      | 查看是否有补丁信息同步任务正在<br>运行。                                     |
| 查看已连接的本地同步服务器 | 查看已经连接至中心服务器的本地<br>同步服务器。                                  |
| 清空补丁记录        | 清空补丁发布列表中的所有补丁配<br>置信息。                                    |

同步日志页面



| 司步日志               | <b>補空日</b> 書  |
|--------------------|---|
| <u>1564</u>        | 西宣  |
| 2009-9-25 23 01:18 | 商車码更新结束   |
| 2009-9-25 23:01:17 | 商審码更新設備下載失敗   |
| 2009-9-25 23:00:19 | 信息同步任务失败:   |
| 2009-9-25 23:00:19 | 关联到YebService(http://patch.patchzource.cm/upservice.ssex)失数 |
| 2009-9-25 23:00:05 | 收到同步任务启动请求,启动同步任务线程成功:                                      |
| 2009-9-25 23:00:05 | 诸求启动计划更新任务。   |
| 2009-9-22 23:00:20 | 发布热修复到补丁管理完成  |
| 2009-9-22 23:00.20 | 没有需要发布的热修复  |
| 2009-9-22 23:00:20 | 没有需要发布的热修复  |
| 2009-9-22 23:00:19 | 信息同步任务成功完成  |
| 2009-9-22 23 00:19 | 开始发布热修复到外丁管理  |
| 2009-9-22 23:00:19 | 查找热修复同步结果:找到0多热修复,0个文件需要下载;                                 |
| 2009-9-22 23:00:17 | 找到147条需要兼除的热频复  |
| 2009-9-22 23:00:05 | 病毒码更新结束   |
| 2009-9-22 23:00:05 | 病毒码更新文件解释完成   |
| 2009-9-22 23:00:05 | 正在处理防病毒软件信息   |
| 2009-9-22 23:00:05 | 病毒研更新数据下载成功,正在处理数据  |
| 2009-9-22 23:00:04 | 收到同步任务启动请求,启动同步任务线程成功:                                      |
| 2009-9-22 23:00:04 | 请求启动计划更新任务。   |
| 2009-9-21 23:54:04 | 病毒码更新结束   |
| 1225               |   |

页面显示了补丁配置库的同步状态,如果同步失败,日志将打印同 步失败的原因。

#### 同步状态页面

| ASHR:  | 2889               | REDE            | HERA        |         |       |       |
|--|--------------------|-----------------|-------------|---------|-------|-------|
| 文件同步   | **                 |                 |             |         |       |       |
| -  | Carte-Serve        | _               | З           |         |       |       |
| 20600  | - NHTH             |                 | Э           |         |       |       |
| LUN  | _                  | _               |             | 20.25   | #7##- | 11/18 |
| 20140  | III Rodeniziti I   | BILLION - AN OR | . 101       | 201700  | 1589  |       |
| DOMAGNET   | 001100-02081       |                 | 1.901       | mach    | 0.649 | 101   |
| Billinde   | Witnestown         | anti-tananti-   | de CE and   |         | 08#   |       |
| minute   | IN ROAMS           | con Dende-      |             |         | CR#   |       |
| (00klade)  | 10140-0001         |                 | 1.107       | 1.040   | CRM   | 1.4   |
| - DESIGN   | OT A sub-states    |                 | 2.00        | 1000    | CRIF. |       |
| (DOALASTY)   | service of the     | 100 We CONT     |             | 3,004   | dile  | 0     |
| 305 hairi-   | OT HUNGED B        | UNDER STREET    |             | 3000    | 0.89  | 0     |
| DER Laute  | and disclosed area |                 | di-CE res   | 3258.05 | CR8   | 9     |
| 0004 Audit   | WTHINGSOM          | 000-000000-     | NY SHI, son | 1044    | diffe | 0     |
| BERNSTE  | COLORADO I         | 81110-48-08     | . 101       | energy  | 1000  |       |
| 1004440  | CITAL AND INCOME.  | SHITE IN CO.    | 1.000       | 100023  | OPP   |       |
| 000Alaulte   | 11/11/4407-10      | 002-01-00       |             | 20000   | 088   |       |
| In the local division of the local divisiono | Contracted 1       | 0010-00-00      | D/          | 71024   | 100   |       |

页面显示了各服务器补丁文件的同步状态,如果同步失败会多次尝 试同步。



## 8.2.3. 配置要点

- 点击"补丁管理-〉在线补丁源-〉系统控制"中"启动同步任 务"的"开始"按钮;
- 点击"在线补丁源->同步日志",确认补丁同日志中无明显的 报错;

| 同步日志 清空            | 日志                     |
|--------------------|------------------------|
| <u>时间</u>          | <u>内容</u>              |
| 2009-9-18 15:27:36 | 找到147条需要删除的热修复         |
| 2009-9-18 15:27:33 | 病毒码更新结束                |
| 2009-9-18 15:27:33 | 病毒码更新文件解释完成            |
| 2009-9-18 15:27:33 | 正在处理防病毒软件信息            |
| 2009-9-18 15:27:33 | 病毒码更新数据下载成功,正在处理数据     |
| 2009-9-18 15:27:30 | 病毒码同步开始                |
| 2009-9-18 15:27:30 | 收到同步任务启动请求,启动同步任务线程成功! |
| 1                  |                        |

点击"在线补丁源->同步状态"查看补丁文件是否均"已同步":

| 系统设置         | 系统控制               | 网络日志            | 同多状态          |         |      |   |
|--------------|--------------------|-----------------|---------------|---------|------|---|
| 200918509-0  | NUVFindors2000-1   | 09711032-s66-CH | S REE         | 1389816 | 己和步  | 0 |
| 2000/#509-6  | 140\Windows2000-3  | 2971032-s00-ES  | V. ECE        | 1382136 | 己购货  | 0 |
| 2000/0509-0  | 040 Windows XP-820 | 71032-#86-CHS   | 424           | 1387376 | 已和新  | 0 |
| 2009/#509-0  | NOWindowsTP-ID     | UNE-38x-22017   | 654           | 1391992 | 己同步  | 0 |
| 2009/MS09-0  | NOWindowsServer    | 2003-10971032-  | 186-CHE. exe  | 1509232 | 己和步  | p |
| 2009/0509-0  | 040\TindowsServer  | 2003-88971032-  | 406-100. este | 1507698 | 己同步  | 0 |
| 2009/4509-0  | 043 WindoesIP-IBI  | 1185T-#86-CHS.  | *2+           | 562032  | 己問步  | 0 |
| 2009/MS09-0  | 141 Windows P-IDI  | T185T-#86-IM/   | 104           | 561529  | 已剩步  | 0 |
| 20091#309-0  | 041 WindowsServer  | 2003-13971657-  | e66-CHS 424   | 554366  | 己阿步  | D |
| 2009/#509-0  | N1WindowsServer    | 2003-10971057-  | 805-110. es a | 553328  | 己同步  | 0 |
| 2009/4509-0  | 141 Windows6. 0-33 | 971657-s00 area |               | 305563  | 己同步  | 0 |
| 2029/#509-6  | 141 Vinderst 0-11  | 971857-186 ara  |               | 308563  | 已罰步  | 0 |
| 2000/#509-0  | 148\VindoenServer  | 2003-88967723-  | 266-CHS +2+   | 845168  | 正在例步 | 0 |
| 2009\#509-0  | 048/WindowsServer  | 2003-33967723-  | 206-200. aza  | 839040  | 正在局步 | 0 |
| 2009/.#209-0 | 10\Tindoes6 0-13   | 967723-x05. mus |               | 4043602 | 正在同步 | 0 |
|              |                    |                 |               |         |      |   |

- 点击"补丁管理->补丁分发->补丁分发->默认分发任务",点
   击应用对象,查看及编辑选择对应的主机名,IP组,用户组和
   工作组;
- 选择补丁安装选项为"自动下载,自动安装",自动下载前提 示用户确认。
- 6. 保存并更新客户端规则。

注意:如果同步日志中有报与服务器连接失败等信息,请重复尝试。



并确认中心服务器到 patch.patchsource.cn 的 80、8800 端口均可达。

**建议:**管理员手工拷贝一份补丁予以备份,方便系统重装或其他测试。

# 8.3. 手工补丁源

## 8.3.1. 关于手工补丁源

- "手工补丁源"作为"在线补丁源"的一种补充,可由管理员 自行配置需要安装的补丁,以满足需要。
- "手工补丁源"发布后补丁分发方式同"在线补丁源"。

#### 名词解释

"**补丁向导"**:添加手工补丁的配置向导,管理员可根据向导指引 一步步完成手工补丁的配置。

### 8.3.2. 配置介绍

| 补丁向导页面   |                  |    |
|----------|------------------|----|
| 系统补丁配置向导 |                  | 帮助 |
| 补丁类型     | Windows系统补丁    ▼ |    |
| 补丁名称     |                  |    |
| 安装顺序号    | 0                |    |
| 描述       | ×                |    |
| 微软安全公告编号 |                  |    |
| 微软安全公告链接 |                  |    |
| 严重程度     | 推荐               |    |
|          | 下一步 取消           |    |





| 补丁类<br>型         | 本系统目前支持 Windows 系统补丁和 IE/Outlook 补丁 两种类型,两种补丁配置的方式不同,请先确认好需要 配置的补丁类型,然后再配置其他选项。  |
|------------------|--|
| 补丁名<br>称         | 输入微软标准的补丁编号,例如 KB824468,Q324567 等,<br>每次只能输入一个。  |
| 安装顺<br>序号        | 本系统在为客户端自动安装补丁时,可设置补丁安装的<br>优先级。此处的安装顺序号数字越小的越优先安装,顺<br>序号的数字不必相连,例如您可以输入10,20,30,<br>100 这样的数字。   |
| 描述               | 微软安全公告中对于此补丁的描述。   |
| 微软安<br>全公告<br>编号 | 发布此补丁的微软安全公告号,例如 MS08-030。   |
| 微软安              | 发布此补丁的微软安全公告的链接,例如   |
| 至公日<br>链接        | /bulletin/ms08-030.mspx。   |
| 严重程<br>度         | 严重程度与微软发布的安全公告的严重等级相对应。  |
| 下一步              |  |
| 文件组<br>名称        | 每个微软公布的补丁都会包含针对不同操作系统或 IE 版本的补丁文件,在此可以添加多个补丁文件组,每个<br>组适用于一种操作系统版本或 IE 版本,其中包含不同<br>语言版本的补丁文件信息。一般补丁文件组以操作系统<br>版本或者 IE 版本来命名。例如在此填入"WinXP",表<br>示本组补丁文件适用于 XP 操作系统。 |
| 自动安<br>装参数       | 补丁自动安装参数,设置补丁采用静默安装的模式,在<br>所有补丁安装完成之前不重新启动操作系统。默认设置<br>为/quiet /norestart,无需修改。   |
| 简体中<br>文版文<br>件  | 填写简体中文版补丁文件存放的相对路径,例如补丁文件存放于服务器安装目录<br>\$/download/AutoUpdate/2008/MS08-008/中,则此处相<br>对路径应该填写:<br>2008\MS08-008\Windows2000-KB943055-x86-CHS.EXE<br>。                |
| 繁体中<br>文版文<br>件  | 填写繁体中文版补丁文件存放的相对路径,填写方式与<br>简体中文版类似。   |
| 英文版<br>文件        | 填写英文版补丁文件存放的相对路径,填写方式与简体<br>中文版类似。   |



| 下一步<br>(类型<br>为<br>Windo<br>ws 系统<br>补丁) |                          |
|--|--------------------------|
| 操作系<br>统                                 | 选择补丁所适用的操作系统版本。          |
| Service<br>Pack                          | 选择补丁所适用的 ServicePack 版本。 |
| 补丁文<br>件组                                | 选择适用的补丁文件组。              |

# 8.4. 补丁分发

### 8.4.1. 关于补丁分发

- "补丁分发"即配置所有终端打补丁的策略。补丁分发可以分为两个阶段,补丁测试与补丁分发。
- 在大规模分发补丁前,可以先在指定的 IP 组中作补丁的测试, 如果确认补丁确实不存在问题,可以结束测试任务并分发。
- "补丁测试"以主机名, IP 组,用户组和工作组为单位,对选定的补丁进行小范围分发测试。所有从补丁源发布的补丁初始状态都是未测试,只有经过测试才会被标记为已测试。
- "补丁分发"以主机名,IP 组,用户组和工作组为单位,对 选定的补丁在设置时间范围内进行分发。状态为未测试和已 测试的补丁都可分发,但建议对所有补丁进行测试后再分 发。
- "分发参数"包括"客户端下载补丁流量"和"是否允许在域 环境下安装补丁"两个选项。

**建议:**虽然天珣补丁已经过严格的测试,但 Windows 补丁自身的问题也可能导致部分终端的蓝屏或死机现象,所以建议大型网



络中对所有的补丁测试。

- "补丁测试"和"补丁分发"可以同时进行,不会出现同一补 丁重复安装的现象。
- ■分发参数 设置客户端下载补丁时的带宽和是否允许在域环境 下安装补丁。

### 8.4.2. 配置介绍



| 配置项:      | 说明              |
|-----------|-----------------|
| 任务名称      | 即补丁测试的名称,以方便管理。 |
| 任务说明      | 填写测试任务的一些补充说明。  |
| 请选择要测试的补丁 | 即选择需要测试的补丁。     |



| 任务状态      | 补丁测试完成后可结束测试任务,即标记为<br>"已完成"。<br>相应的补丁状态为"已测试"。  |
|-----------|--|
| 补丁安装选项    | 即补丁的安装方式,可以手工安装("不自动<br>下载"),可以"自动下载,手工安装",可以<br>"自动下载,自动安装",也可以"静默下载,<br>静默安装",并且可以根据需要"自动下载前<br>提示用户确认"。 |
| 补丁安装前的提示信 | 在这里填写提示信息,那么在安装补丁前,  |
| 息         | 就会弹框提示相关文字信息。  |
| 补丁安装完成的提示 | 在这里填写提示信息,补丁安装完成之后,  |
| 信息        | 则会弹框提示相关文字信息。  |
| 应用到 IP 地址 | 在这里可以输入单个 IP 地址,也可以输入某<br>个 IP 组里面的 IP 地址范围。   |
| 应用对象      | 点击"查看及编辑"超链接,选择测试补丁<br>的主机名, IP组,用户组和工作组。  |

补丁分发页面

| ▶丁分 <b>发</b><br>54-8和 |                                    |                  |  |          |      |
|-----------------------|------------------------------------|------------------|--|----------|------|
| 424                   | 54555584+26<br>801174968394<br>87- | 条。创新新发<br>则这个分发任 | 1  |          |      |
| 18月第1920日丁            | NHTGIER                            |                  |  |          | 0.77 |
|                       | · P# 0000                          | PROSESSAT        | 需要被 Second 叶丁                                  | #316-511 |      |
|                       | -                                  | ICROMENT         | Provide Scite # 1999年中的講道可能导致代码的外位             | 8/06-014 |      |
|                       | -                                  | 1000018459 T     | RESERVOIRSEBRIESCRIGENING                      | 681-03   |      |
|                       | ·                                  | VERNER (R) T     | 工具管理操作的最美可能均可补行性的                              | #34-019  |      |
|                       | PE DOUD                            | KORONE AND T     | 在高计划程序中的重要可能化作用任何                              | REBA-COL | ¥-   |
|                       | · ····                             | CHORE & MINT     | IN. ABHORADING AND A                           | 6084-025 | Φ.   |
|                       | ·                                  | IDENTESSIT       | Findowy Shall Philipping Sciences              | R104-424 |      |
|                       | ·                                  | VURNERSHIT       | Table 10. Series Soller 1982 Still BERTERN "EM | 8081-000 |      |



| 市产属于都非丁和高        | HHE CA      | H Martine           | BADRING . |  |
|------------------|-------------|---------------------|-----------|--|
| 84#S             | -           |                     |           |  |
| 科丁安制造项           | 不自动下数       | <ul> <li></li></ul> | CBMB/MB/  |  |
| NTEMMERTO        |             |                     |           |  |
|                  |             |                     |           |  |
| HT TON ALCORNALS |             |                     |           |  |
| O'EN#            | (正宗軍臣明文祖用刘贵 | > 262mm             |           |  |
| 1400+Rox0al      | E           |                     |           |  |
|                  | 0(1) W.S    | 1                   |           |  |

| 配置项:           | 说明   |
|----------------|--|
| 任务名称           | 即补丁测试的名称,以方便管理。  |
| 任务说明           | 填写测试任务的一些补充说明。   |
| 请选择要测试的补丁      | 即选择需要测试的补丁。  |
| 客户端下载补丁时间      | 配置补丁分发时间范围。  |
| 任务状态           | 补丁测试完成后可结束测试任务,即标记为<br>"己完成"。<br>相应的补丁状态为"己测试"。  |
| 补丁安装选项         | 即补丁的安装方式,可以手工安装("不自动<br>下载"),可以"自动下载,手工安装",可以<br>"自动下载,自动安装",也可以"静默下载,<br>静默安装",并且可以根据需要"自动下载前<br>提示用户确认"。 |
| 补丁安装前的提示信<br>息 | 在这里填写提示信息,那么在安装补丁前,<br>就会弹框提示相关文字信息。   |
| 补丁安装完成的提示信息    | 在这里填写提示信息,补丁安装完成之后,<br>则会弹框提示相关文字信息。   |
| 应用对象           | 点击"查看及编辑"超链接,选择测试补丁<br>的主机名,IP组,用户组和工作组。   |



系统"默认分发任务":自动处理的分发任务,该任务将自动同步所有补丁,管理员仅需将所有 IP 组加入该分发任务即可实现补丁的自动分发。如果需要测试补丁和定期分发补丁,可以将"默认分发任务"的"任务状态"改为"已终止"。

#### 分发参数页面

| 补丁分发参数          |     | <u>帮助</u> |
|-----------------|-----|-----------|
| 补丁分发参数 <b>:</b> |     | <u>修改</u> |
| 客户端下载补丁流量       | 不限制 |           |
| 是否允许在域环境下安装补丁   | 不允许 |           |

| 配置项:              | 说明                            |  |
|-------------------|-------------------------------|--|
| 客户端下载补丁流量         | 可实现客户端下载补丁的流量限制,也可以<br>不限制带宽。 |  |
| 是否允许在域环境下<br>安装补丁 | 该参数支持补丁在域环境下安装                |  |

# 8.5. WSUS 集成管理

## 8.6. 关于 WSUS 集成管理

- "WSUS 集成"在策略服务器端配置 WSUS 补丁更新策略并下发 至客户端,由客户端自动修改补丁更新相关的组策略和注册 表项,然后利用 WSUS 系统自动分发微软各种补丁。
- 天珣客户端分发 WSUS 补丁是利用 Windows System Update 功能实现,而分发"在线补丁"是利用天珣自身的补丁精灵客户端实现。
- "WSUS 补丁源"利用天珣客户端的部署同时通过策略配置终端的 WSUS 选项,免去了 WSUS 客户端的部署麻烦。
- "WSUS 补丁源"和"在线补丁源"的补丁分发方式不同,



可以一起配置相互作为补充。参见《天珣典型配置示例文 档》。

#### 名词解释

"WSUS "是 Windows Server Update Services 的简称,可以更新 Windows 补丁,同时具有报告功能,管理员还可以控制更新过程。 WSUS 是个微软推出的网络化的免费的补丁分发方案,可以在微 软网站上去下载。WSUS 支持微软公司全部产品的更新,包括 Office、SQL Server、MSDE 和 Exchange Server 等内容。通过 WSUS 这个内部网络中的 Windows 升级服务,所有 Windows 更 新都集中下载到内部网的 WSUS 服务器中,而网络中的客户机 通过 WSUS 服务器来得到更新。这在很大程度上节省了资源, 避免了资源浪费并且提高了效率。

**"WSUS 补丁源"**: 天珣客户端可以代替 WSUS 客户端负责补丁的分发策略配置。

### 8.6.1. 配置介绍

| 常規画法<br>Latrase更新原表(EL<br>Latrase(第十原表(EL<br>を増えの更新 |  |
|---|--|
| Intrase更新服务的L<br>Intraset的计服务的L                     |  |
| Late and 我计服务 (BL                                   |  |
| ATR ALL PAGE  |  |
| i i   | 佛知下就未満如安寨<br>1987年前37年前半村安央时,下唐協會要祝春<br>1985年前期 年代<br>1985年前月間 (12):111  |
| 6   | 1至又再此现于执行计划的重新目动自己还要新导持的而高。数以值25分钟1 计中间中的值2~1,440分平<br>1至又在最终执行计划的重新启动相目动更新导导的时间,意以值2分钟1 计中间有效值1~20分钟1   |
| GOURGE S  | IX HR/東部県市北京市市市市市市市市市田田田市(1500年第11月間時時的時間) 分野(高加加)~60分钟)<br>北洋市島Intrant Winterst世界期間市局定面の高名内容<br>北洋市営営業局局「加強支援機構な<br>算止防安日助営業会員<br>大洋市営業品の自己資産設立局交換<br>(1148月日本部分部分局交換<br>第211日の日本部分部分局交換<br>(1148月日本部分部分局交換<br>(1148月日本部分部分局交換<br>(1148月日本部分部分局交換<br>(1148月日本部分部分局交換<br>(1148月日本部分部分局交換<br>(1148月日本部分部分局交換<br>(1148月日本部分部分)<br>(1148月日本部分部分)<br>(1148月日本部分部分)<br>(1148月日本部分部分)<br>(1148月日本部分部分)<br>(1148月日本部分部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148月日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日日本部分)<br>(1148日本部分)<br>(1148日日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本部分)<br>(1148日本<br>(1148日本)<br>(1148日本<br>(1148日本)<br>(1148日本<br>(1148日 |
| <b>客户端目标组</b>                                       | 1.光平常戶編首任台灣  |
| 自定文目动更新检测频率<br>(数以最221年)                            | 「 后間 小村 (荷地道) (22 (村))   |
| 自在2.845年4月前月末<br>第八章21年1                            | 北井県戸藤田 存在2<br>  后間   |

#### WSUS 集成管理页面



| 策略名称              | 建议 WSUS 服务器的名称,以便于管理。  |
|-------------------|--|
| Intranet 更新服务 URL | 填写补丁更新服务的URL,例如安装<br>更新服务的服务器 IP 地址为<br>192.168.0.11,则更新 URL 为<br><u>http://192.168.0.11</u> 。   |
| Intranet 统计服务 URL | 填写补丁统计服务的 URL,例如安装<br>统计服务的服务器 IP 地址为<br>192.168.0.11,则统计 URL 为<br><u>http://192.168.0.11</u> 。  |
|                   | 配置客户端补丁自动更新时的下载<br>和安装的方式,此处可以有四种选<br>择:"通知下载并通知安装"、"自动<br>下载并通知安装"、"自动下载并计划   |
| 配置自动更新            | <b>安装"、"允许使用本地管理员的设</b><br>置",只有在选择"自动下载并计划<br>安装"时,才会激活计划安装相关的<br>详细配置。   |
| 配置自动更新<br>自动更新选项  | 安装"、"允许使用本地管理员的设置",只有在选择"自动下载并计划<br>安装"时,才会激活计划安装相关的<br>详细配置。<br>设置 WSUS 客户端获取补丁自动更新<br>的扩展选项,例如允许来自 Intranet<br>Microsoft 更新服务器位置的签名内<br>容,允许非管理员接收更新通知,计<br>划的自动更新安装完成后不自动重<br>新启动等。 |



|                               |  | 组中。   |
|-------------------------------|--|---|
| 自定义自动                         | 更新检测频率(默   | 设置客户端向 WSUS 服务器检测补丁                               |
| 认值 22 小时                      | <sup>+</sup> )   | 更新的频率。  |
| 生如时间                          | 新有时间 包工作时间   | 10 非工作时间 10 以下时间段                                 |
|                               | 开始时间   | 結束対何 載報 ■除<br>■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ |
| 在线模式                          | 开始时间<br>又在线时生效 又高线时  |   |
| 在线模式<br>策略应用对象                | 开始时间<br>「日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日  | 结皮时间 編編 圖版<br>                                    |
| 在线模式<br>策略应用对象<br>创建类型        | 开始时间<br>「「「「「「」」」」」」<br>「「「「」」」」」<br>「「「」」」」」<br>「「「」」」」」<br>「「」」」」<br>「「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」」<br>「」」」<br>「」」」」<br>「」」」」<br>「」」」<br>「」」」」<br>「」」」<br>「」」」」<br>「」」」」<br>「」」」<br>「」」」」<br>「」」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」」<br>「」」」」<br>「」」」<br>「」」」」」<br>「」」」<br>「」」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」<br>「」」」<br>「」」」」<br>「」」」<br>「」」」」<br>「」」<br>「」」」<br>「」」」<br>「」」」」<br>「」」<br>「」」」<br>「」」」<br>「」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」<br>「」」」<br>「」」」<br>「」」」<br>「」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」<br>「」」」<br>「」」」<br>「」」」<br>「」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」<br>「」」」<br>「」」」<br>「」」<br>「」」<br>「」」」<br>「」」<br>「」」<br>「」」<br>「」」」<br>「」」<br>「」」」<br>「」」」<br>「」」」<br>「」」<br>「」」」<br>「」」」<br>「」」」<br>「」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」」<br>「」」」<br>「」」<br>「」」」<br>「」」」<br>「」」」<br>「」」」<br>「」」<br>「」」」<br>「」」」<br>「」」<br>「」」」<br>「」」<br>「」」<br>」<br>「」」<br>「」」」<br>「」」<br>「」」<br>「」」<br>」<br>「」」」<br>「」」」<br>「」」<br>「」」<br>「」」<br>「」」<br>」<br>」<br>」<br>」<br>「」」」<br>「」」<br>」<br>」<br>」<br>」<br>」<br>」<br>」<br>」<br>」<br>」<br>」<br>」<br>」<br>」<br>」<br>」<br>」<br>」<br>」 | 结束时间 編編 圖版<br>                                    |
| 在线模式<br>策略应用对象<br>创建类型<br>创建者 | 开始时间<br>学 在线时生效 学 高线时的<br>《 还没有应用到任何对象 》<br>全局<br>jing   | 结皮时间  |

| 配置项:   | 说明                                   |
|--------|--------------------------------------|
| 生效时间   | 目前策略的生效时间可以灵活配置,可<br>以根据管理员的需求进行配置。  |
| 在线模式   | 策略运行的方式有客户端在线和离线两<br>种模式。            |
| 策略应用对象 | 策略应用对象有四种方式:基于主机名,<br>IP 组,用户组,和工作组。 |

**建议:**分发 WSUS 补丁需要管理员对补丁测试,建议不要在生产终端、财务终端 IP 组中启用 WSUS 补丁管理。

## 8.6.2. 配置要点

 1、添加"WSUS补丁策略"输入"策略名称"、"描述"、"Intranet 更新服务 URL"、"Intranet 统计服务 URL"。示例如下图:



| ₩SUS补丁策略        |                                       | <u>帮助</u> |
|-----------------|---------------------------------------|-----------|
| 策略名称            | 信息中心sus服务器(161)                       | *         |
| 描述              | 信息中心测试的₩SUS服务器,ip地址为<br>192.168.0.161 | ×         |
| Intranet更新服务URL | http://192.168.0.161                  | *         |
| Intranet统计服务URL | http://192.168.0.161                  |           |

2、 点击"策略应用对象"的"查看及编辑"超链接,添加需要补

丁分发的 IP 组并"确定",如下图:

| WSUS集成管 | <u>5理</u>    |
|---------|--------------|
| WSUS集成  | <b>这管理</b>   |
| 对象类型    | IP组 Z 全部选中   |
| 对象选择    | 🗖 xin        |
|         | <b>确定</b> 取消 |
|         |              |

3、 客户端更新规则。

# 8.7. 补丁查询

## 8.7.1. 关于补丁查询

- "补丁查询"为管理员提供了补丁分发结果的查询窗口,可以 根据补丁查询结果,总结补丁管理的效果并提交补丁管理的 报表。
- "从电脑查补丁"确定指定终端上的补丁安装情况。
- "从补丁查电脑"确定指定补丁部署情况。

**说明**:补丁信息由客户端报表统一上报,补丁上报周期同客户端 报表上报周期。



## 8.7.2. 配置介绍

### 从电脑查补丁页面

| 配置项: 说明  |
|--|
| <ul><li>输入需要查询补丁安装状态的电脑</li><li>请输入要查询的 IP 地址</li><li>的 IP 地址,此电脑必须已经安装本</li><li>系统的客户端。</li></ul> |

#### 从补丁查电脑页面

| 从补丁查电脑            |         |           |
|-------------------|---------|-----------|
| 请输入补丁号<br>请选择查询类型 | ▼求安装已安装 | <u>帮助</u> |
| 请选择IP组            | 信息中心    | 查询        |
| IP地址              |         |           |
| 1                 |         |           |

| 配置项:    | 说明   |
|---------|--|
| 输入补丁号   | 输入标准的补丁编号,例如<br>KB861112。                                |
| 请选择查询类型 | "要求安装"表示该补丁存在于补丁<br>分发任务内,系统会自动向客户端分<br>发。"强制要求安装"表示该补丁存 |
|         | 在丁安全状态的补丁强制规则内,系<br>统将此补丁作为安全状态选项,强制<br>客户端安装。           |



请选择 IP 组

选择补丁查询的范围。

# 9.资产管理

# 9.1. 关于资产管理

资产管理依托于天珣客户端,收集内网终端的所有资产信息,包括

软、硬件信息。

| 与出到Eacal<br>共1委記录           | 1                 |                |       |           |       |     | đ  | MARACO MO           |
|-----------------------------|-------------------|----------------|-------|-----------|-------|-----|----|---------------------|
| 12 18 1                     | 84-18.16          | 156            | 174   | B0.55     | 0.010 | 100 |    | 1.0000              |
| 1961, 1881, 1991, 1997<br>1 | 00-28-18-68-40-63 | windPD-linesis | teri) | Tindor II | estet | 100 | R. | 2012-11-14 05:57.28 |

默认进入页面时会显示所有已经上报过资产的终端的概况。显示为 绿色的资产信息为有发生过资产变更的终端。可通过右上角的部门 选择栏选择想要查询的部门中的终端资产信息,并可通过"导出到 excel"按钮形成报表。

#### 资产信息

要查看某台终端的资产详细信息,可以点击其 IP 地址进入资产信息明细页面



| ACT:         | 资产信息              |   |
|--------------|-------------------|---|
| 管理           | <b>萤</b> 严Ⅲ       | (988CT98A-AABA-4216-8349-DTA7D3A36506)      |
| 10년<br>15月3日 | 主机名               | winMP3-lizemin                              |
| 存錄           | 操作系统              | Findows SP                                  |
| e車)ナ<br>前法雑  | 主机类型              | 笔记本   |
| 管理           | cnu数号             | Intel (K) Core (TM)2 Duo CPU T5070 0 2.0036 |
| 中心           | 硬盘序列号             | WD-#XE046913896                             |
| 00.05        | 阿卡nac线址           | 00-26-18-67-40-63                           |
| 策略<br>9530   | 计算机序列号 (58)       | 4019255212F2D9781AR                         |
| 地面           | <b>是否安装了多操作系统</b> | 4   |
| s.           | 所應部门              | 未定义朝门                                       |
|              | 使用人               |   |
|              | WPGD MM           | 西北市市出作 删除资产信息                               |

#### 点击"资产信息明细"按钮,可查看该终端详细的资产信息

| http://192.168.1.209.8033/PM/Web/w   | settoroniser appx%/apse                         | HD = (980 C79FA AABA 4216-8349-D7A7D3A30506-6ArsetSH+ & ShoregeD #+ & fu |
|--|---|--|
| B#18: (988070PA-AABA-4216-   | 8349-DTATD3A3651                                | 86)  |
| <ul> <li>(资产信息)</li> <li>□ 硬件</li> </ul>   | 58  | fictoroft Kinders 27 Professional  |
| BIOS<br>处理器<br>主板  | NE<br>1958/17                                   | r#98   |
| CD-10.00<br>显示<br>紅小48   | 数号<br>5時<br>(1)第日                               | vidP2-li (min  |
| 电池<br>= 输入   | 地動内存<br>用户名                                     | almonistrator  |
| ED HA  | NI-   | a l  |
| * 増口<br>存補<br>資卡<br>()<br>()<br>()<br>()<br>()<br>()<br>()<br>()<br>()<br>()<br>()<br>()<br>() | 名称<br>新本<br>原基性新本<br>空间助影内存<br>空间改图空间<br>空间虚拟内存 | Bieronaft Tindow IF Froferniand  |
| 采载周安战  | 安熱时间<br>制造度<br>名称<br>注册用户                       | 2011-1-5 12:35:02  |
|  | 序列号<br>系统延动器                                    | ADDRESS/IPTEW791AE   |
|  | 系统目录  |  |

点击"**查看变更事件**"按钮,即可查看该终端变更事件明细表



| 资产信息 资产              | <b>使更亊件</b>  |
|----------------------|--|
| 是否安装了多操作系统           | 是  |
| 所属部门                 | 未定义部门  |
| 使用人                  |  |
| 资产信息明细               | <b>防查</b>  |
| 347 IN 16 7144       |  |
|                      |  |
| 亦再 中心                |  |
|                      |  |
| 2012-10-30 8:20:07   | <br>Microsoft Visual Studio Macro Tools 安装   |
| 2012-10-30 8:20:07   | Microsoft Visual Studio Macro Tools - CHS Language Pack 安<br>裝                               |
| 2012-10-30 8:20:07   | Fences 安装  |
| 2012-10-30 8:20:07   | Microsoft Help Viewer 1.1 <b>安装</b>  |
| 2012-10-30 8:20:07   | Microsoft .NET Framework 4 Extended 安装   |
| 2012-10-30 8:20:07   | Microsoft .NET Framework 2.0 安装  |
| 2012-10-30 8:20:07   | Microsoft .NET Framework 4 Client Profile 安装   |
| 2012-10-30 8:20:07   | Microsoft Visual Studio 2010 Tools for Office Runtime<br>(x86) 安装                            |
| 2012-10-11 9:22:30   | Microsoft Visual Studio 2010 Tools for Office Runtime<br>(x86) Language Pack - CHS <b>安装</b> |
| 2012-10-11 9:22:30   | Microsoft Visual Studio 2010 Tools for Office Runtime<br>(x86)语言包 - 简体中文 <b>安装</b>           |
| 1 2 3 4 5 6 7 8 9 10 | ! <u></u>  |
|                      |  |

点击"删除资产信息"按钮,则该终端的资产会被删除.删除后,

下一次客户端会重新上报该终端的资产信息

| 资产信息                                  |                               |                                     |
|---------------------------------------|-------------------------------|-------------------------------------|
| 第 <b>严</b> 口                          | (980CT0FA-AADA-4216-8040-0    | TATDIARMONG)                        |
| 王机名                                   | einW2-lizezin                 |                                     |
| 操作系统                                  | Findows XP                    |                                     |
| 王机共型                                  | 笔记丰                           |                                     |
| CLORE &                               | Intal (B) Core (TR)2 Das (TFF | TT070 & 2.000Hz                     |
| 硬盘序均导                                 | #D-%2E046913896               |                                     |
| 阿卡里尼達拉                                | 00-28-18-69-40-63             | Windows Internet Explorer           |
| 计算机序列号(580)                           | 4379255212F2D97E1AB           | (?) 当前选择资产信息以及历史记录、支票事件记录将按量除。是否继续: |
| 是否安装了多操作系统                            | 4                             | × .                                 |
| 所議察门                                  | 未定义部门                         |                                     |
| 使用人                                   |                               |                                     |
| · · · · · · · · · · · · · · · · · · · | AZAZ00                        | 1時後方後日                              |

#### 资产变更事件

如果客户端发生了硬件或软件变更,天珣将会自动记录其变更信 息,并在此进行查询



| 【产交更事件<br>140.72597 -                                    |           | sama il | · · · · · · · ·   | 97 HHMT   |
|--|-----------|---------|-------------------|---|
|  | ±#/6      | 1711    | 1100              | 12  |
| n anne an ac-ar traintail                                | jantar ar | v       | 20141 11 11 20    | GRAND CHL ACAUST 200 2 MADES dis Arread<br>Because on a sources)<br>위해 또한 Acaust 200 Acaust 200 Acaust 200<br>위해 한다. Acaust 200 Acaust 200 Acaust 200<br>(200 Acaust 200 Acaust 200 Acaust 200 Acaust 200<br>(200 Acaust 200 Acaust 200 Acaust 200 Acaust 200<br>(200 Acaust 200 Acaust |
| TRUCK ALL ALL AND ALL ALL ALL ALL ALL ALL ALL ALL ALL AL | 11-009-11 | 188     | 3002-012 18:59-51 | HE DOMESTICS IN STATISTICS  |

管理员可以通过查询变更事件,准确掌握硬件和软件资产的变动情况。

# 10. 非法外联

# 10.1. 关于非法外联

非法外联控制示意图



■天珣防止"非法外联"控制分五个层面:"非法外联监控"、"多

网卡限制"、"拨号限制"、"外设管理"与"异常路由审计"。
 ■禁用移动存储设备的写入操作包括外设管理中禁用移动设备,
 移动存储驱动禁止移动设备 IO 流写入(允许读数据)两个

层面。禁止移动设备 IO 流写入配置参见《用户手册-移动存储章节》。



- ■异常路由审计结果在"信息中心->外联监控->异常路由查询" 中体现。
- ■非管理手段干预的前提下,非法外联控制的前提是天珣各种准 入控制,只有保证网络中所有终端均强制安装天珣客户端才 能完全杜绝非法外联行为。

**注意:"安全防护->防护策略"**的离线禁止网络访问策略经常用 于非法外联环境中,但不属非法外联范畴。具体参见《用户手册 -安全防护->防护策略->访问控制章节》。

### 名词解释

- "非法外联":指内网终端非法利用各种外设或网络技术连接 至其他网络或拷贝数据的行为。这种行为有意或无意的成为 了内网安全的漏洞,甚至数据泄密。
- "非法外联监控":用于实现对终端非法外联行为进行监控, 并对非法外连行为进行告警或者是阻止,并告知管理员。
- "多网卡限制":天珣客户端保护连接至内网的网卡,屏蔽掉 其他网卡的数据可防止内网终端通过其他网卡非法外联的 行为。
- "拨号限制":用于对客户端的拨号连接进行限制,主要的限制类型有 PPP 拨号、PPPoE 拨号和 VPN 拨号。
- "外设管理":用于对终端外设的使用进行控制,禁用或者是
   6用某个特定或者某些外接设备。
- "异常路由审计":内网环境特点决定了内网终端路由信息相对无变化。但非法连接其他网络或代理上网将导致路由信息的变化,通过路由信息的变化,可以定位非法外联的网络行为。



# 10.2. 非法外联监控

## 10.2.1. 配置介绍

非法外连监控通过监控终端探测网络的两种方式(分别为 ping 和 telnet)来控制终端访问网络的行为,当监控到有非法外联行为产 生时,可以记录非法外联行为,向客户端告警、向管理员发送告警 信息(非法外联行为上传到服务器/短信/邮件通知等)、断开客户端 网络等方式进行告警和阻止。

#### 非法外联监控

点击"非法外联监控"标签中的"添加"按钮





| 配置项:   | <u>说明</u>  |
|--------|--|
| 策略名称   | 此处填写策略名称如"test"  |
| 策略描述   | 对策略进行描述,或备注等   |
| 探测方式   | 这里选择检查网络非法外联的方式<br>(ping 或 telnet)   |
| 探测目标列表 | 此处填写用来检测网络连接的探测目标<br>ip 或域名。注:如选择 telnet 方式,请<br>先确认探测目标允许 telnet 连接,可以<br>填写多个探测目标。 |
| 动作     | 此处选择检测到非法外联行为后执行的<br>动作:1、记录非法外联行为(默认启用);<br>2、客户端告警;3、向管理员发送告警;<br>4、断开网络。          |
| 在线模式   | 配置此策略在在线和离线时是否生效   |
| 生效时间   | 可以根据管理员的需求,灵活配置策略<br>生效的时间范围。  |
| 策略应用对象 | 目前策略应用对象有四种:基于主机名,<br>IP组,用户组,和工作组。  |

非法外联告警设置



非法外联监控 非法外联告警设置

#### 非法外联告警设置

| 非法外联告警设置:  |             | 修改 |
|------------|-------------|----|
| 汇总告警时间     | <b>0</b> 分钟 |    |
| 蜂鸣器告警秒数    | 0秒          |    |
| 邮箱服务器地址    |             |    |
| 用户名        |             |    |
| 登录密码       |             |    |
| 发送邮箱地址     |             |    |
| SMTP服务器端口  |             |    |
| 告警时接收的邮箱地址 |             |    |
| 告警时接收的手机号码 |             |    |

#### 点击**非法外联告警设置:"修改"**按钮

| 非法外联监控 非法外联告警设置         |          |        |
|-------------------------|----------|--------|
| 非让从联生敬识罢                |          |        |
| 非位外收口言义且                |          |        |
| 汇总告警时间(*若填空或为0则不告警)     | 0        | 分钟     |
| 蜂鸣器告警长响(*若填空或为0则不启用蜂鸣)  | 0        | 秒      |
| 邮箱服务器地址(*若填空则不发邮件)      |          |        |
| 用户名(*若填空则不发邮件)          |          |        |
| 登录密码                    |          |        |
| 发送邮箱地址                  |          |        |
| SMTP服务器端口(*若填空则不发邮件)    |          |        |
|                         | *        |        |
|                         |          |        |
| 告警时接收的邮箱地址(*若填空则不发邮件)   |          | 测试邮箱用户 |
|                         |          |        |
|                         | <b>T</b> |        |
|                         | <u>^</u> |        |
| 生物时均收的毛机呈现(*类病参加)学校病(含) |          |        |
| 古客时接收的于机亏碍( 石壤呈则不及超信)   |          |        |
|                         |          |        |
|                         | 保存返回     |        |

| 配置项:    | <u>说明</u>              |
|---------|------------------------|
|         | 此处设置汇总告警时间间隔,填(*若填空    |
| 汇共使中间   | 或为0则不告警);如:设置汇总时间为1分钟, |
| 化忍口害的问  | 则一分钟汇总一次告警信息,然后以信息形式   |
|         | 发送到手机或邮箱               |
| 蜂鸣器告警长响 | 此处设置告警时,蜂鸣器鸣响时间(*若填    |
|         | 空或为 0 则不启用蜂鸣器)注: 需硬件支持 |



| 邮箱服务器地址    | 此处填写用来发送告警邮件的邮箱服务<br>器地址(*若填空则不发邮件)                 |
|------------|---|
| 用户名        | 此处填写用来发送告警邮件的邮箱登录<br>名(*若填空则不发邮件)                   |
| 登录密码       | 此处填写邮箱地址对应的密码                                       |
| 发送邮箱地址     | 此处填写发送告警邮件的邮箱地址,例:<br>mj@163.com                    |
| SMTP 服务器端口 | Smtp 服务器端口,常见如 25,,993…<br>(*若填空则不发邮件)              |
| 告警时接收的邮箱地址 | 用来接收告警邮件的邮箱地址,可填写<br>多个,一行一个。(*若填空则不发邮件)            |
| 告警时接收的手机号码 | 用来接收告警短信的手机号码,可填写<br>多个,一行一个。(*若填空则不发短信)注:<br>需硬件支持 |

# 10.3. 多网卡限制

# 10.4. 关于多网卡限制

- "多网卡限制"用于限制内网终端同时连接多个网络的行为。
- "多网卡限制"分为允许网卡切换和禁止网卡切换两种场景,
   场景区别在于内网应用场景是否单一。
- "多网卡限制"在禁止使用多网卡的前提下,能够允许使用指 定的"非物理网卡",以满足各种应用场景。
- ●存在一种特殊场景,内网中部分用户可以访问指定网络资源, 而另一部分用户无法访问该资源。可以访问该网络资源的用 户为不能访问该资源的用户提供网络代理。此行为可通过 "网站访问控制与审计"中"禁止使用 HTTP 代理服务器上



网"结合非法路由审计功能解决。

**说明**: Windows 网络共享上网需要多网卡,故与禁止 HTTP 代理 上网有别。

**重点**:网络行为的非法外联控制不仅仅需要多网卡控制,更严格的内网非法外来控制还需要禁止离线客户端访问任何网络,禁止离线客户端使用外设和移动存储设备以及离线审计等策略。

#### 名词解释

"拨号网卡(PPP, VPN, PPPOE)等":调制解调器、ADSL、 VPN 等各种行为,存在各种拨号网卡负责数据发送,而某些场景 下这种行为是合法性的外联行为,天珣允许对该设备单独做例外排 除。

"虚拟网卡(虚拟机)": VMware 等虚拟机将创建特殊的虚拟网卡, 而这些网卡在宿主终端上属多网卡,因此部分合法应用需要做例外 排除。

"物理网卡":具有硬件实体的网卡,比如有线以太网卡、无线网卡等。 "非物理网卡":由程序创建的用于特殊环境的虚拟网卡,比如 PPP 拨号、PPPOE 拨号、VPN 拨号,虚拟机虚拟网卡。

说明:Windows 系统不分物理网卡和非物理网卡,其接口完全相同。 不同网卡由天珣安全内核驱动识别。

### 10.4.1. 多网卡限制页面

#### 配置介绍



| 27C-40-1010 | *   |
|-------------|---|
| 策略描述        |   |
| 限制多网卡       | <ul> <li>         允许在所有活动网卡间切换(包括物理网卡和非物理网卡)     </li> <li>         不允许在物理网卡间切换,以下非物理网卡始终可用         允许在物理网卡间切换,以下非物理网卡始终可用         加卡在物理网卡间切换,以下非物理网卡始终可用         加卡名·贝PP, VPN, PPPDP等)         加卡名·贝PP, VPN, PPPDP等)     </li> </ul> |
| 生效时间        | <ul> <li>●所有时间</li> <li>● 工作时间</li> <li>◎ 非工作时间</li> <li>◎ 以下时间段</li> <li>开始时间</li> <li>结束时间</li> <li>结束时间</li> <li>结索</li> <li>2012-05-10</li> <li>35.00</li> <li>2012-05-10</li> <li>131:30</li> <li>55.00</li> </ul>               |
| 在线模式        | 🔽 在线时生效 🔽 离线时生效   |
| 策略应用对象      | (还没有应用到任何对象) 查看及编辑  |
| 创建类型        | 全局  |
| 创建者         | jing  |

| 配置项:  | 说明  |
|-------|---|
| 策略名称  | 输入合适的策略名称,以方便管理。  |
| 限制多网卡 | <ul> <li>默认只有第一个连通到策略服务器的网卡才可以通讯,其他的网卡都不允许通讯。</li> <li>"允许在所有活动网卡间切换(包括物理网卡和非物理网卡)":如果选中这个选项,客户端"切换网卡"菜单将激活,用户可在所有可用的网卡中选择一个网卡通信,没有被选中的网卡不能通信。</li> <li>"不允许在物理网卡间切换,以下物理网卡始终可用":如果选中这个选项,客户端"切换网卡"菜单不激活,系统只允许第一个连通到策略服务器的物理网卡以及下面选中的非物理网卡通信,其他的网卡不能通信。</li> <li>"允许在物理网卡间切换,以下非物理网卡</li> </ul> |
|       | 始终可用":如果选中这个选项,客户端"切  |
|       | 换网卡"菜单将激活,用户可在可用的物理   |
|       | 网卡中选择一个网卡通信,没有被选中的物   |
|       | 理网卡不能通信,同时下面选中的非物理网   |



|        | 卡也可以通信。  |
|--------|--|
| 生效时间   | 可以根据管理员的需求,灵活配置策略生效<br>的时间范围。                              |
| 在线模式   | 在线时生效,客户端处于在线状态时该规则<br>生效,离线时生效,客户端处理离线状态时<br>该规则生效,默认均选中。 |
| 策略应用对象 | 目前策略应用对象有四种:基于主机名, IP 组,用户组,和工作组。                          |

### 配置要点

1. 点击"添加"多网卡限制策略,如下图:

| 箫略夕称               |   |
|--------------------|---|
| ₩ <b>₩8-₩3</b> -₩3 | *   |
| 策略描述               |   |
| 限制多网卡              | <ul> <li>⑦ 允许在所有活动网卡间切换(包括物理网卡和非物理网卡)</li> <li>⑧ 不允许在物理网卡间切换,以下非物理网卡始终可用</li> <li>◎ 允许在物理网卡间切换,以下非物理网卡始终可用</li> </ul> |
| 生效时间               | 🔝 拨号网卡(PPP,VPN,PPPOE等) 📄 虚拟网卡(虚拟机)  |
|                    | 💿 所有时间 🔘 工作时间 🔘 非工作时间 🔘 以下时间段   |
|                    | 开始时间 结束时间 编辑 删除   |
|                    | 2012-05-10 9:00 2012-05-10 19:00 适加   |
| 在线模式               | ☑ 在线时生效 ☑ 离线时生效   |
| 策略应用对象             | (还没有应用到任何对象) 查看及编辑  |
| 创建类型               | 全局  |
| 创建者                | jing  |
| 注・左进右∗号的顶          | 日心须经》   |

点击"策略应用对象"->"查看及编辑"超链接,关联指定的
 IP 组,如下图。选择指定的 IP 组,并"确定":



| 多网卡限制 |              |
|-------|--------------|
| 多网卡限  | 制            |
| 对象类型  | IP组 ▼ 全部选中   |
| 对象选择  | 🗖 xin        |
|       | <b>确定</b> 取消 |

3. "保存"并更新客户端规则。

# 10.5. 拨号限制

- 10.5.1. 关于拨号限制
  - "拨号限制"分为禁止 PPP 拨号,禁止 PPPoE 拨号,禁止 VPN 拨号。满足不同环境下对多网卡外联的全面管理。禁止 PPP 拨号 不仅能对 PPP 连接进行限制,也能根据需求对指定号码进行限制。
    - 说明:关于长途号码,如果"区号"或"国家(地区)代码"
       中有一个不为空就认为是长途号码。

### 10.5.2. 拨号限制页面

配置介绍



| 拔号限制                   |  |
|------------------------|--|
| 拨号限制                   |  |
| 策略名称                   | *  |
| 策略描述                   |  |
| 拔号类型限制                 | □ 禁止PPP(传统MODEM)拨号   |
|                        | □ 禁止PPP₀E (ADSL、3G等) 拨号  |
|                        | □禁止VFN(虚拟专用网)拨号  |
| 拨号号码限制<br>(針对PPP拨号)    | 🔲 禁止拨长途号码(包括国内和国际)   |
| (1)/311110(-5)/        | □ 禁止拨以下列表中的号码  |
| 生效时间                   | <ul> <li>毎个号码一行,可以输入多个号码。</li> <li>● 所有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段</li> <li>开始时间</li></ul> |
| 在线模式                   |  |
| 策略应用对象                 | ■ 12:844J エ XX ■ 商 584J エ XX (   |
| ж <del>ч</del> ыхлилык |  |
| 创建类型                   | 全局   |
| 创建者                    | jing   |
| <b>注:右边有∗号的项目</b> 必须   | 页输入。<br>【 <b>保存】 取消</b>  |

| 配置项:   | 说明  |
|--------|---|
| 策略名称   | 输入合适的策略名称,以方便管理。  |
| 策略描述   | 对策略的备注,及详细内容描述等   |
| 拨号类型限制 | <ul> <li>禁止 ppp(传统 modem)拨号,勾选此项可以禁止所有的 ppp拨号连接。</li> <li>禁止 PPPoE(ADSL、3G等)拨号,勾选此项可以禁止所有的 PPPoE拨号连接。</li> <li>禁止 VPN(虚拟专用网)拨号,勾选此项可以禁止所有的 VPN拨号连接。</li> <li>注:三个选项可以复选,勾选禁止 ppp拨号后,拨号号码限制不可选。</li> </ul> |
| 拨号号码限制 | ◆ 禁止拨打长途号码(包括国内和国际),  |



|        | 勾选此项,可以禁止拨所有的国内国外     |
|--------|-----------------------|
|        | 长途号,但允许拨短途或者是内线号。     |
|        | ◆ 禁止拨打以下列表中的号码, 勾选此处, |
|        | 只对列表中的号码进行限制。         |
|        | 注:可以复选,勾选拨以下列表中的号码后,  |
|        | 可以对列表进行编辑,每个号码一行,可以   |
|        | 输入多个号码。               |
| 生效时间   | 可以根据管理员的需求,灵活配置策略生效   |
|        | 的时间范围。                |
|        | 在线时生效,客户端处于在线状态时该规则   |
| 在线模式   | 生效,离线时生效,客户端处理离线状态时   |
|        | 该规则生效,默认均选中。          |
| 策略应用对象 | 目前策略应用对象有四种:基于主机名, IP |
|        | 组,用户组,和工作组。           |
|        | 1                     |

#### 配置要点

#### 4. 点击"添加"拨号限制策略,如下图:

| 拨号限 <del>制</del>    |  |
|---------------------|--|
| 策略名称                | *  |
| 策略描述                | А.<br> <br>  т   |
| 拔号类型限制              | □ 禁止PPP(传统MODEM)拨号   |
|                     | □ 禁止PPP₀E (ADSL、3G等)拨号   |
|                     | □禁止VPN(虚拟专用网)拨号  |
| 拨号号码限制<br>(针对PPP拨号) | 🔲 禁止拨长途号码(包括国内和国际)   |
|                     | □禁止拨以下列表中的号码   |
|                     |  |
| 生效时间                | 每个号码一行,可以输入多个号码。   |
| 1.0011-1            | <ul> <li>所有时间</li> <li>工作时间</li> <li>非工作时间</li> <li>以下时间段</li> </ul> |
|                     | 开始时间 结束时间 编辑 删除  |
|                     | 2012-05-10 9:00 2012-05-10 13:30 護加                                  |



| 在线模式                     | 📝 在线时生效 📝 离线时生效           |
|--------------------------|---------------------------|
| 策略应用对象                   | (还没有应用到任何对象) <u>查看及编辑</u> |
| 创建类型                     | 全局                        |
| 创建者                      | jing                      |
| 注:右边有*号的项目必须输入。<br>保存 取消 |                           |

- 点击"策略应用对象"->"查看及编辑"超链接,关联指定的
   IP 组,选择指定的 IP 组,并"确定":
- 6. "保存"并更新客户端规则。

# 10.6. 外设管理

### 10.6.1. 关于外设管理

- "外设管理"可以最大限度的控制系统外设,杜绝各种非法外联的外设。
- "外设管理"中原有规则禁用外设后,除非将规则更改为启用 该外设,否则该外设将保持被禁用状态。

**建议:**配置设置禁用规则后,相应配置一条外设启用规则,如果 需要取消外设禁用则将 IP 组改为启用外设的规则中。详细操作 见《本节配置要点》

#### 名词解释

"设备采样": 以某个 IP 地址终端的外设为基线,确定需要启用 或禁用的外设。

### 10.6.2. 外设管理页面

#### 配置介绍



| *####   |  |
|---|--|
| 外设管理  |  |
| NESS  | •  |
| 策略論述  |  |
| 瀬用内遺设書  | ND 単行口 (208日)<br>F 通貨解消費<br>2番 元規時千  |
| ■算牙设备<br>第用USP设备<br>■例解和USP设备 ■ USP服務/機会 ■  | 「移动硬盘(0盘) 【 鼠标/健盘/0盘之外的056设备   |
| 其它需要管理的设备   | <b>教育集加 ···</b>  |
|   |  |
| 在納機式. ジ 正純的主法 ジ 案純的主法<br>効率回用対象 ( 近然有回用影性相対象 ) <u>数素可编辑</u><br>创建共型 全局<br>加維者 jus<br>注: 右边有+号的項目の学編入。<br>一個在 服務 |  |
| 配置项:  | 说明   |
| 策略名称  | 输入规则的名称,以便于管理。   |
| 策略描述  | 对策略的备注,及详细内容描述等  |
| 禁用内置设备以及禁用 USB 设  | 管理员可以根据需求,勾选上需要禁   |
| 备   | 用的设备。  |
|   |  |
|   | 通过采样某个终端的外设,在输入框   |
| 其他需要管理的设备   | 通过采样某个终端的外设,在输入框<br>内输入该终端的 IP 地址,选择需要禁  |
| 其他需要管理的设备   | 通过采样某个终端的外设,在输入框<br>内输入该终端的 IP 地址,选择需要禁<br>用的设备。   |
| 其他需要管理的设备<br>注:没有被勾选上的其他设备,影  | 通过采样某个终端的外设,在输入框<br>内输入该终端的 IP 地址,选择需要禁<br>用的设备。<br><b>状认会被启动</b>  |
| 其他需要管理的设备<br>注:没有被勾选上的其他设备,颗  | 通过采样某个终端的外设,在输入框<br>内输入该终端的 IP 地址,选择需要禁<br>用的设备。<br><b>大认会被启动</b><br>可以根据管理员的需求,灵活配置策  |
| 其他需要管理的设备<br>注:没有被勾选上的其他设备,颗<br>生效时间  | 通过采样某个终端的外设,在输入框<br>内输入该终端的 IP 地址,选择需要禁<br>用的设备。<br><b>状认会被启动</b><br>可以根据管理员的需求,灵活配置策<br>略生效的时间范围。   |
| 其他需要管理的设备<br>注:没有被勾选上的其他设备,影<br>生效时间  | 通过采样某个终端的外设,在输入框<br>内输入该终端的 IP 地址,选择需要禁<br>用的设备。<br><b>大认会被启动</b><br>可以根据管理员的需求,灵活配置策<br>略生效的时间范围。<br>在线时生效,客户端处于在线状态时                     |
| 其他需要管理的设备<br>注:没有被勾选上的其他设备,影<br>生效时间<br>在线模式  | 通过采样某个终端的外设,在输入框<br>内输入该终端的 IP 地址,选择需要禁<br>用的设备。<br><b>大认会被启动</b><br>可以根据管理员的需求,灵活配置策<br>略生效的时间范围。<br>在线时生效,客户端处于在线状态时<br>该规则生效,离线时生效,客户端处 |


|        | 中。                                    |
|--------|---------------------------------------|
| 策略应用对象 | 目前策略应用对象有四种:基于主机<br>名, IP 组,用户组,和工作组。 |

"设备采样",选择需要禁用的终端外设。

在地址框中输入需要采样的 IP 地址,对其进行驱动采样:

|  | 终端取样咨询结果   |            |    |
|--|--|------------|----|
|  | 保存选择的项目  | 保存所有的项目    | 关闭 |
|  | ₩ 设备名案   | 识别标志       |    |
|  | 🔲 Wicrosoft AC Adapter   | CnBatt     |    |
|  | Intel (R) Core (IM)2 Du<br>CPU T5870 @ 2.00GHz                               | o intelppm |    |
|  | Intel(R) Core(TM)2 Du<br>CPU T5870 @ 2.00GHz                                 | o intelppm |    |
|  | ThinkPad UltraMay<br>Pointing Device   | i8042prt   |    |
|  | ThinkPed PM Device for<br>SL Series  | r IBMPNDRV |    |
|  | Standard 101/102-Key<br>or Microsoft Natural<br>PS/2 Keyboard with HP<br>QLB | i8042prt   |    |
|  | PCI bus  | pei        |    |
|  | Microsoft ACPI-<br>Compliant Embedded<br>Controller                          | ACPIEC     |    |

勾选设备并确定后即可对其进行采样,并加入到控制的外设列表中:





# 10.7. 异常路由审计

# 10.7.1. 关于异常路由审计

"异常路由审计页面"即异常路由审计配置页面,输入正确的
 网关用以标记异常的路由信息。只需要将正常的默认网关在
 此作汇总即可。

# 10.7.2. 异常路由审计配置页面

### 配置介绍

| 异常路由审计     |          |         |     |  |
|------------|----------|---------|-----|--|
| 当前管理网段 初始管 | 理网段 添加 1 | 北量添加 返回 |     |  |
|            |          |         |     |  |
| 默认网关地址     | 阿关描述     | 创建状态    | 创建者 |  |
| 1          |          |         |     |  |

| 配置项:   | 说明                                    |
|--------|---------------------------------------|
| 选择服务器  | 选择需要维护的服务器。                           |
| 选择管理网段 | 选择需要维护的管理网段                           |
| 添加     | 添加正确的默认网关的 IP 地址                      |
|        | 如果您的网络中每个子网的网关 IP 非                   |
|        | 常有规律,您可以通过批量添加的方                      |
|        | 式,一次添加多个网关 IP 地址。如果                   |
|        | 您的子网网关分别为10.0.0.1,                    |
| 批量添加   | 10. 0. 1. 1, 10. 0. 3. 110. 0. 20. 1, |
|        | 您可以通过批量添加,在起始网关地址                     |
|        | 填 10.0.0.1, 在结束网关地址填                  |
|        | 10.0.20.1,系统将自动为您添加 21                |
|        | 个网关地址。                                |



# 11. 移动存储

# 11.1. 关于移动存储

- "移动存储"管理与"外设管理"共同对移动存储设备进行控制。
- 未启用"移动存储"管理的网段使用移动存储设备不受限制。对 启用了"移动存储"管理的网段,设置基本参数。对于每一个移 动存储设备的认证和授权,请在"设备授权"—>"移动存储设 备授权" 中设置。

**说明**:移动存储设备的 GUID 号 是不同的移动存储设备之间相互区 分的唯一标识。

- "分区加扰"用于对数据拷贝性能要求高的环境中,设备中的数据 并未做加密,但对设备分区表做了加密,导致未授权的终端无法 打开该移动存储设备。
- "目录加密"模式中移动设备原理上不需要格式化,但新购买的移动存储设备建议格式化后对其认证并授权。
- "全盘加密"用于对整个磁盘内的数据加密,未授权的移动存储介 质无法访问。

**注意**:天珣未改动移动存储设备硬件的任何信息,原理上不会导致 移动设备损坏的现象,但建议对移动存储设备中的**数据做可靠备份**。

■在"外设管理"对移动存储设备的控制为启用的情况下,设备受移动存储管理策略的控制。下图是移动存储设备使用权限表。

| "外设管理" | "外设管理"不对移动存储设备进行控制 |
|--------|--------------------|
| 禁用移动存储 |                    |

| 设备      |           |        |           |         |
|---------|-----------|--------|-----------|---------|
| 1、移动存储设 | 受移动存储策略管理 |        |           |         |
| 备不能使用   | 不启用移动存    | 启用移动存储 | 管理的网段     |         |
| 2、移动存储设 | 储管理的网段    |        |           |         |
| 备策略不能生  | 1、网段未被关   | 网段被关联到 | 」某一个移动存储管 | 营理策略    |
| 效       | 联到任何移动    | 设备无需认  | 设备需认证     |         |
|         | 存储管理策略    | 证      |           |         |
|         | 2、移动存储设   | 任何用户按  | 设备使用情况    | 受认证及授权状 |
|         | 备的使用不受    | 照"不对移  | 态决定       |         |
|         | 任何限制      | 动存储设备  | 未认证的设     | 已认证的设   |
|         |           | 进行认证   | 备         | 备       |
|         |           | 时,对移动  | 1、在允许使    | 1、授权的登  |
|         |           | 存储设备的  | 用未认证设     | 录用户根据   |
|         |           | 使用权限"  | 置的电脑上     | 授权使用    |
|         |           | 使用     | 可以使用      | 2、未授权的  |
|         |           |        | 2、其他电脑    | 用户无权使   |
|         |           |        | 禁止使用      | 用       |

**建议:** 新购移动存储设备确保已格式化,避免设备量产时未设置磁盘 卷标。

- ■"设备认证策略": 设置移动存储设备的认证策略并关联相应的
   IP 组,使策略生效。
- "移动存储设备授权":用户提交移动存储设备的认证后,该设备出现在此列表中。系统管理员对设备进行认证并授权用户使用该移动存储设备的权限。
- "未认证设备的使用授权":对于某些电脑,可以使用未经认证的移动存储设备。当客户端弹出移动存储设备认证窗口时,用户可点击"不认证"。



# 11.2. 设备认证策略

## 11.2.1. 关于设备认证策略

- 同一移动存储设备只能有一种认证策略,即"移动存储设备管理
   策略"认证策略为单选,一个 IP 组只能存在于一种 "移动存储
   设备管理策略"。
- 全盘加密时,可以支持多分区大容量移动存储设备,但格式化设 备需要较长的时间。

#### 名词解释

"设备认证策略":即移动存储设备的认证策略,此策略包含对 "移动存储设备管理策略"的选择,以及该策略应用到的 IP 组范 围。

"移动存储设备管理策略":即移动存储设备的认证方式、是否加密、是否禁用、是否只读、是否读写等。

"专用目录加密认证" : 此种认证方式会生成一个名为加密目录 的文件夹。加密目录内的数据已加密,但名称未加密;加密目录外 的数据未加密。已授权的设备可读取所有数据;未授权的设备取法 读取任何目录。未安装天珣客户端的设备只可查看加密目录外的数 据;加密目录内的数据呈乱码,不能查看。

"全盘加密认证":整个磁盘内的数据加密,加密算法为 AES-256。 未授权的移动存储介质无法访问,已授权的移动存储介质由天珣客 户端格式化己加密分区。磁盘中的数据由天珣客户端负责加密存盘 以及解密读入内存。未安装天珣客户端的终端无法打开磁盘,无法 读取己加密数据。

**注意:**尽管已对数据存取做了性能优化,但全盘数据加密必然导致大文件拷贝的速率降低。全盘加密的时耗为140%左右。



"分区加扰认证":磁盘分区被加密,但并未对磁盘数据做加密。 未授权的移动存储介质无法访问,已授权的移动存储介质由天珣客 户端格式化已加密分区。未安装天珣客户端的终端无法打开磁盘, 无法读取数据。

## 11.2.2. 移动存储设备提交认证相关页面

| , µц | AH 1 121. |                               |   |
|------|-----------|-------------------------------|---|
| 移动存  | 储管理       |                               | × |
| Ť    | 设备名称:     | Kingston DT 101 G2 USB Device |   |
|      | 责任人:      |                               |   |
| ļ    | 归属部门:     | Υ.                            |   |
|      | 电话:       |                               |   |
|      | Email :   |                               |   |
|      | IP地址:     | 192.168.1.152                 |   |
|      | 主机名:      | winXP3-lizexin                |   |
|      | 提交认证      | 不认证 取消                        |   |

 1、未认证的移动存储设备插入受控终端,弹出移动存储认证页 面,如下图:

 2、提交认证但未授权的移动存储设备插入受控终端时,弹出系统 提示:"管理员正在处理,移动存储设备\*\*\*暂时不能使用", 如下图:





 3、提交认证并仅授予读的权限时,插入移动存储设备,弹出系统 提示:"你对移动磁盘\*\*\*的非加密目录没有写权限,加密目录 没有写权限"(此处以专用加密目录认证为例)。

| 移动存储   | X |
|--|---|
| 客户端状态提示  |   |
| 您对移动磁盘Kingston DT 101 G2 USB Device-662的非加密<br>目录没有写权限,加密目录没有写权限 |   |
|  |   |
| 查看更多   |   |

4、已提交并授权的移动存储设备插入受控终端,就会去策略服务 器查询是否有相应的GUID,如果此时受控终端的网络不通,30 秒超时,则会根据离线授权弹出提示;若此时没有离线授权, 系统则会根据设备的认证策略弹出提示,如:认证策略是:专 用目录加密,弹出的提示"你对移动磁盘 XXX 的加密目录和 非加密目录没有访问权限";如果是全盘加密,提示则相应的 变为"你对移动磁盘 XXX 没有访问权限"。专用目录提示如下 图:





# 11.3. 移动存储设备管理页面

### 配置介绍

移动存储设备管理策略配置页面如下:

| 移动存储设备认证策略   |                  |
|--------------|------------------|
| 移动存储管理       |                  |
| 策略名称         | *                |
| 策略描述         |                  |
| 移动存储设备使用策略   | ◎ 禁止使用           |
|              | ◎ 设备只读           |
|              | 🔘 设备可读写          |
|              | ● 专用目录加密认证       |
|              | ◎ 全盘加密认证         |
|              | ⑦分区加扰认证          |
| 在线模式         | ☑ 在线时生效 🗵 离线时生效  |
| 策略应用对象       | 查看及编辑            |
| 创建类型         | 全局               |
| 创建者          | jing             |
| 注:右边有*号的项目必须 | 须输入。<br>保存 删除 取消 |
| 配置项:         | 说明               |



| 策略名称           | 输入合适的策略名称,以方便管理。  |
|----------------|---|
| 移动存储设备使用策<br>略 | 选择移动存储的使用策略,属单选类型。  |
| 在线模式           | 移动存储设备无离线模式,故默认强制<br>均选中。   |
| 策略应用对象         | 点击"查看及编辑"超链接,选择指定的 IP<br>组,工作组,主机名,或者用户组,则这些<br>对象中的电脑启用移动存储设备使用策略。 |

注意:"禁止使用"、"设备可读"、"设备可读写"、与"外设管理" 的区别在于此处是由天珣移动存储驱动控制。"专用目录加密认 证"、"全盘加密认证"、"分区加扰认证"参考<u>《本节名词解释》</u>

### 配置要点

1、专用目录加密认证配置
 点击"添加"移动存储设备管理策略,选择"专用目录加密认证",如下图:



| 移动存储设备认证策略  |  |
|-------------|--|
| 移动存储管理      |  |
| 策略名称        | 专用目录加密认证 *                                 |
| 策略描述        |  |
| 移动存储设备使用策略  | <ul> <li>◎ 禁止使用</li> <li>◎ 设备只读</li> </ul> |
|             | <ul> <li>设备可读写</li> </ul>                  |
|             | ◉ 专用目录加密认证                                 |
|             | ◎ 全盘加密认证                                   |
|             | ◎ 分区加扰认证                                   |
| 在线模式        | 🗹 在线时生效 🔽 离线时生效                            |
| 策略应用对象      | 查看及编辑                                      |
| 创建类型        | 全局   |
| 创建者         | jing                                       |
| 注:右边有*号的项目必 | 须输入。<br>保存 删除 取消                           |

2、 点击"策略应用对象"->"查看及编辑"超链接,关联指定的

| 移动存储设备                    | <mark>认证策略</mark> |
|---------------------------|-------------------|
| 移动存储<br><sub>专用目录加密</sub> | <b>管理</b><br>认证   |
| 对象类型                      | IP组 Z 全部选中        |
| 对象选择                      | 🖉 xin             |
|                           | <b>确定</b> 取消      |

IP组,如下图。选择指定的IP组,并"确定":

"保存"并更新客户端规则。



# 11.4. 设备授权

# 11.4.1. 关于设备授权

- "设备授权":即对移动存储设备或对可使用未认证设备的计算机授权。
- "移动存储设备授权": 用于对未认证的移动存储设备在线授权。
- "可使用未认证设备的计算机":指移动存储设备策略特殊的环境中,对指定计算机做例外排除,这些计算机可以读取已认证磁盘和未认证磁盘。
- ■授权页面相关名词解释:

"未认证":移动存储设备没有经过认证。

- "已经认证":移动存储设备经过了管理员的认证。
- "只授权不加密":只对移动存储设备授权,但并没有对其进行加密,已安装天珣客户端并授权的计算机对该移动存储设备的读写权限是根据操作权限中设置的权限而定;未安装天珣的计算机能够任意读写移动存储设备内的数据;已安装天珣客户端但未授权的计算机不能访问该移动存储设备。

## 11.4.2. 移动存储设备授权页面

#### 配置介绍

| P#49        | 8/1 (H##1) | 1812 | THE THE | - 1    |           |         |
|-------------|------------|------|---------|--------|-----------|---------|
| 重型法中设备 就是找收 | BG ARMEN   |      |         |        |           |         |
|             | 1002071    |      | LINA.   | PROVID | 0.0410.00 | INCOME. |

"移动存储设备授权"页面中列出来了所有未认证和已认证的设备

供管理员在线授权,具体参考配置要点。



### 配置要点

| 移动存储管理  |                               |
|---------|-------------------------------|
| 设备名称:   | Kingston DT 101 G2 USB Device |
| 责任人:    |                               |
| 归属部门:   | 4                             |
| 电话:     |                               |
| Email : |                               |
| IP地址:   | 192, 168, 1, 152              |
| 主机名:    | winXP3-lizexin                |
| 提交认证    | 不认证 取消                        |

1、未认证的移动存储设备插入受控终端,弹出移动存储认证页面,

如下图:

2、由用户填写标记该移动磁盘的相关信息,包括责任人,部门、
 IP 地址、主机名等,并以电话等方式申请管理员授权。

**注意:**每一次提交认证成功,将会触发策略服务器同步策略, 不用去手动同步。

3、管理员确认该移动存储设备合法性,并授权。如下图:

下图为专用目录加密授权页面:



| 移动存储设备授权  | 可使用未认证设备的计算机                                |
|-----------|---|
| 移动存储设备持   | 2 <b>权</b> (同一个U盘加密模式更改后,请删除该U盘对应的旧认证及授权信息) |
| 设备编号      | Kingston DT 101 G2 USB Device-662           |
| 部门        | * 选择部门                                      |
| 责任人       | lzx *                                       |
| 主机名       | win%P3-lizexin                              |
| IP地址      | 192. 168. 1. 152                            |
| 授权状态      | ◎ 未授权 ● 授权通过 ◎ 只授权不加密                       |
| 加密模式      | 专用加密目录                                      |
| 非加密目录操作权限 | ■读 ■写 ■离线读 ■离线写                             |
| 加密目录操作权限  | ■读 ■写 ■离线读 ■离线写                             |
| 申请认证时间    | 2012-10-30 8:20:21                          |
| 应用对象授权    | 查看及编辑                                       |
|           | 保存 圖除 取消                                    |

下图为全盘加密授权页面:

| 移动存储设备授权 | 可使用未认证设备的计算机                               |
|----------|--|
| 移动存储设备持  | <b>受权</b> (同一个U盘加密模式更改后,请删除该U盘对应的旧认证及授权信息) |
| 设备编号     | Teclast CoolFlash USB Device-996           |
| 部门       | * 选择部门                                     |
| 责任人      | abc *                                      |
| 主机名      | winXP3-lizexin                             |
| IP地址     | 192. 168. 1. 152                           |
| 授权状态     | 💿 未授权 💿 授权通过 🔵 只授权不加密                      |
| 加密模式     | 全盘加密                                       |
| 操作权限     | □读 □写 □离线读 □离线写                            |
| 申请认证时间   | 2012-10-30 8:37:22                         |
| 应用对象授权   | (还没有授权到任何对象) <u>查看及编辑</u><br>保存 圖除 取消      |

下图为分区加扰授权页面:



| 移动存储设备授权 | 可使用未认证设备的计算机                        |
|----------|-------------------------------------|
| 移动存储设备指  | 受权 (同一个U盘加密模式更改后,请删除该U盘对应的旧认证及授权信息) |
| 设备编号     | Teclast CoolFlash USB Device-424    |
| 部门       | * 选择部门                              |
| 责任人      | abc *                               |
| 主机名      | win%F3-lizexin                      |
| IP地址     | 192. 168. 1. 152                    |
| 授权状态     | ◎ 未授权 ● 授权通过 ◎ 只授权不加密               |
| 加密模式     | 分区加扰                                |
| 操作权限     | ■读 ■写 ■离线读 ■离线写                     |
| 申请认证时间   | 2012-10-30 8:39:33                  |
| 应用对象授权   | (还没有授权到任何对象) <u>查看及编辑</u>           |
|          |                                     |

4、将授权信息下发到指定的终端 IP 组,主机名,工作组,或者用 户组,例:点击 "应用对象授权" 后的"查看及编辑"超链 接,弹出授权信息,如下图:

| 移动存储设备        | 授权 可使用未认证设备的计算机                      |
|---------------|--------------------------------------|
| 移动存储          | 设备授权(同一个U盘加密模式更改后,请删除该U盘对应的旧认证及授权信息) |
| Teclast Coolf | 'lash USB Device-424                 |
| 对象类型          | IP组 Z 全部选中                           |
| 对象选择          | <b>xin</b>                           |
|               | <b>瑜定</b> 取消                         |

授权信息下发到指定用户组的操作参照上述第4点。

"保存"。

**说明1**: 授权保存后,客户端不用去手动更新策略,也可以获得相应的认证策略信息,但新的认证策略只会对下次接入的移动存储设备生效,对于已接入的移动存储设备必须重新接入才会获得新的认证策略,上述情况只对所属服务器是中心服务器的客户端而言。对于所属服务器是本地服务器的客户端,如果在提交认证开始一分钟之内就授权完成,则自动会将认证信息和授权信息一起同步到本地



服务器;如果提交认证一分钟之后提交授权信息,则必须先同步一 下本地服务器的策略,客户端才会自动获取相应的认证策略信息。

**说明 2:** 如果授权信息中有离线授权,则缓存授权信息;如果授权 信息中没有离线授权,则删除本地缓存的授权信息。

# 11.5. 可使用未认证设备的计算机

如果需要对一些受控终端进行特别例外,使其可以使用未认证过的 U 盘的话,则可以在此进行配置。

### 配置介绍

| 移动存储设备领权 <mark>可使用未认证</mark> 在                       | 音的计算机 | <u> </u> |            |       |       |                           |
|--|-------|----------|------------|-------|-------|---------------------------|
| 可使用未认证设备的计算机<br>———————————————————————————————————— | itte. |          |            |       |       |                           |
| 097  |       | WITE S   | TAC IN CO. | mitta | MEA   | Contraction of the second |
|  |       |          |            | A.10  | 1.0.1 | 14                        |

如需要批量添加客户端,可以点击"从文件导入"将大量客户端信息导入进来,省却了单独配置的麻烦。当然也可以将已配置好的信息导出作为备份。

**说明**:终端识别号是天珣客户端自动注册时,服务器为其分配的唯一的序列号。

#### 配置要点

1、点击"添加"可使用未认证设备的计算机,弹出如下图:



| 客户端查询   |           |   |         |
|---------|-----------|---|---------|
| 组合查询条件: | 只从客户端报表查询 |   |         |
| 所属IP组   | **请选择**   | × |         |
| IP地址    |           |   | (可模糊查询) |
| MAC地址   |           |   | (可模糊查询) |
| 主机名     |           |   | (可模糊查询) |
| 每页显示行数  | 20        | × |         |
|         | 查询 全部重设   |   |         |

2、选择所属的 IP 组并查询,得到终端的查询结果,如下:

| # 21 | 朱光荣 國由國        | CALIFIC MAL |                |                                    |             |     |
|------|----------------|-------------|----------------|------------------------------------|-------------|-----|
| 127  | A 17784        | 计线发天世       | THE            | eurs.                              | #IEC===91   | RC. |
| 12   | 172.20.2.117   | ΨT.         | 101-1300004004 | D4111407-500-600-306-34400900861   | HOUMDING    |     |
| 1    | UTL 20. 49. 25 | ŦI          | 1200008-230707 | (CONTRACTOR - CON- AND CONTRACTOR) | 172.25.84.+ |     |
| 13   | 10.0.11.0      | ₩£,         | stamin.        | 0000000-009-004-006-004096014941   | (72.01.04.+ |     |

3、选中需要授权的终端,并点击"保存所选的计算机"。

| P-0开展设备放权 ····································         | <u>III.</u> |         |        |        |        |
|--|-------------|---------|--------|--------|--------|
| 可使用未认证设备的计算机 运<br>———————————————————————————————————— |             |         |        |        |        |
|  |             |         |        |        | - 27 6 |
| 0.901  | 计算机的        | BAC MEN | MILLIO | 0182-5 | 1177   |

4、当移动设备接入这些例外的计算机时,会弹出一个认证框:

| 设备名称:       | Pedest CoolPlesh USB Device                    |
|-------------|--|
| 责任人:        |  |
| 白尾窓门:       |  |
| 电话:         |  |
| Enal 1      |  |
| 即地址:        | 192, 168, 133, 1527eclast CoolPlash US5 Device |
| 主机名:        | wir0/P3-lizexin                                |
|             |  |
| 18.17.12.10 |  |



点击"**不认证**"时,则可以直接使用接入的移动设备,而不需要提 交认证授权。

# 11.6. 分区解扰操作说明

- 天珣客户端可以针对分区加扰的移动存储设备进行解扰。
- ■分区解扰需要输入策略服务器帐号和密码确认身份,即仅提供在 线解扰。
- 分区解扰后的移动设备为普通移动存储设备。
- 分区解扰操作将提供分区解扰审计。

### 配置要点

打开客户端安装目录(%program files%\venustech\endpoint security\escc),如下图:



2、打开 PTDecrypt 程序,如下图:



| 管理员帐户: |      |    |   |  |
|--------|------|----|---|--|
| 密码:    | -    |    | - |  |
|        | 7.2  |    |   |  |
|        | 7% = |    |   |  |
|        | 登录   | 退出 |   |  |

3、输入管理员的帐号和密码,即登录 Web8833 的用户名和密码。

该帐号必须具有分区解扰的权限,如下图:

### 系统操作员

| 系统操作员名称:    | jian     | •       |                  |  |
|-------------|----------|---------|------------------|--|
| 系统操作员全名:    | jian     | •       |                  |  |
| 是否敢活:       | ◎否◎是     |         |                  |  |
| 是否是只读权限:    | ●否○是     |         |                  |  |
| 是否全筹管理员:    | 白苦患者     |         |                  |  |
| 是否按需支援管理员境: | ⊙否●是 Î   | ] 保持需支援 | 管理员端,不能登录z+b管理界面 |  |
| 资产管理权限:     | ◎光◎只读●完全 | ei空®]   | □ 只能管理资产         |  |
| 分区解扰:       | ◎ 不能 ● 能 |         |                  |  |
|             |          |         |                  |  |

#### 4、输入用户名和密码和进入解扰页面:

|    |      | 读取已 | 已加扰的移动盘 |     |    |
|----|------|-----|---------|-----|----|
| 扁号 | 设备名称 |     | 大小(MB)  | 盘符  | 状态 |
| .0 |      |     | NL.     | NG. | la |
|    |      |     |         |     |    |
|    |      |     |         |     |    |
|    |      |     |         |     |    |
|    |      |     |         |     |    |

5、如果移动盘未加扰,显示状态为未加扰:



|             | 读取已加               | 加扰的移动盘  |     |                   |
|-------------|--------------------|---------|-----|-------------------|
| 编号   设备名称   |                    | 大小 (MB) | 盘符  | 状态                |
| . Jeclast C | OTLTERU ODB DEALCE |         | 340 | э <b>т</b> елини. |
|             |                    |         |     |                   |

6、如果移动盘已加扰,显示状态为已加扰:

|    | 续取已                            | 加加的移动量  |     |      |
|----|--------------------------------|---------|-----|------|
| 備号 | 设备名称                           | 大小(008) | 盘符  | 状态   |
| 1  | Teclast Coolflash USB Device : |         | 128 | Entr |
|    | HMBR                           | e       | 出   |      |

7、对于已加扰的移动存储设备,选中后点击"**开始解扰"**。如图:

|                                    | 读取已加扰的移动盘         |    |                  |
|------------------------------------|-------------------|----|------------------|
| 扁号   设备名称<br>Toclast Coolflash USB | 大小 (MB)<br>Nevice | 盘符 | <b>状态</b><br>已加拔 |
|                                    |                   |    |                  |

# 12. 终端审计

# 12.1. 关于终端审计

- 审计信息较多,为减轻审计信息上报对网络的影响,天珣客户端
   每二十条审计信息上报一次,低于 20 条审计信息,暂时缓存至
   本地磁盘。
- 同一时间,同一审计信息将拒绝多次插入数据库,仅记录该审计 条目的并发次数。



因审计数据过多,配置审计策略后建议同时配置数据库维护策
 略,详见《用户手册-数据库维护章节》。

**注意**:本章节介绍终端审计策略的配置页面,终端审计信息的查询请 查询"信息中心-审计信息"。

因攻击告警服务器的启动依赖于 SQL Server 的启动,故服务器操作系统重启时可能会出现 SQL Server 启动过慢导致攻击告警服务无法启动的现象。

建议:因审计数据内容将占有大量磁盘空间,建议在安装天珣策略服务器前确保 SQL Server 数据库磁盘空间至少有 40G 空间。

- "终端审计":关于终端审计策略配置和各审计内容的控制策略的配置。
- "文件审计及控制":关于系统磁盘资源,网络资源相关的审计
   策略配置和各资源路径及目录控制策略的配置。
- "打印审计及控制":可以对共享打印机、网络打印机等行为控制 或审计,但不审计打印内容,审计的信息包括:打印机名称、文 档名称、IP 地址、MAC 地址、主机名、用户名、页数和打印时 间。
- "网站审计及控制":即基于 HTTP 原语,对 URL 信息做控制与 审计。可以对 URL 的关键字控制与审计,但不能对 WEB 页面 内容做审计。可以控制 WEB 代理的行为,也可以对合法 WEB 代理做例外排除。
- "FTP 审计及控制": 即基于 FTP 协议的基础上,对终端 FTP 传输行为进行审计,并将这些审计信息上传给服务器。可以对 FTP 的关键字控制及审计,也可以限对终端访问 FTP 服务器及



其端口进行控制。

- "文件涉密信息审计": 对于系统磁盘资源的内容进行审计,但 不对系统磁盘资源的名称或者是目录进行审计,可以添加多个审 计关键字。
- "应用程序使用审计": 对终端运行程序运行行为进行审计,即 可以对指定的某个进程或某些进程进行审计,也可以对终端运行 的多有程序进行审计;策略配置后,应用程序开启,关闭后,就 会审计下该应用程序运行的状态,包括开始关闭的时间及共运行 的时间。
- "刻录审计":支持对终端刻录行为进行控制及审计,并上报审计 信息到服务器。
- "Windows 事件日志审计": 能够审计到终端用户 windows 应用 程序日志、安全日志、系统日志并发送到服务器。

# 12.2. 文件审计及控制策略

## 12.2.1关于文件审计及控制策略

- 文件审计可以针对系统中指定文件夹进行审计,例如:C:\temp 目录。
- 配置控制文件的写入策略时,如果拒绝读取和写入系统关键目 录,将导致系统蓝屏或死机。
- 文件目录审计的配置支持系统环境变量,支持的环境变 量: %ProgramFiles%, %windir%。

- "审计所有移动盘":对 U 盘、USB 移动硬盘等相关 USB 移动 磁盘的审计策略配置和控制策略的配置。可以针对"文件名关键 **字"、"进程名"**做审计和控制。
- "审计所有本地盘":关于系统所有分区的审计策略配置和控制 263



策略的配置。可以针对"**文件名关键字"、"进程名"**做审计和控制。

- "审计网络拷贝":网络拷贝即拷贝网络中的共享文件,共享文件源于远端共享服务器。"审计网络拷贝"即对拷贝其他终端共享的数据做审计。
- "审计共享目录":共享目录即本机的共享文件夹,共享文件夹中的数据源于本地磁盘。"审计共享目录"即审计其他终端访问本机的共享目录。文件属本地磁盘,可以对共享目录中的数据做操作控制。

注意:注意选择包含子目录,否则审计文件夹下的子目录将无审计。

# 12.3. 文件审计及控制策略

## 13.2.1关于文件审计及控制策略

- 文件审计可以针对系统中指定文件夹进行审计,例如:C:\temp
   目录。
- 配置控制文件的写入策略时,如果拒绝读取和写入系统关键目
   录,将导致系统蓝屏或死机。
- 文件目录审计的配置支持系统环境变量,支持的环境变量:%ProgramFiles%,%windir%。

- "审计所有移动盘":对 U 盘、USB 移动硬盘等相关 USB 移动
   磁盘的审计策略配置和控制策略的配置。可以针对"文件名关键
   字"、"进程名"做审计和控制。
- "审计所有本地盘":关于系统所有分区的审计策略配置和控制 策略的配置。可以针对"文件名关键字"、"进程名"做审计和控



制。

- "审计网络拷贝":网络拷贝即拷贝网络中的共享文件,共享文件源于远端共享服务器。"审计网络拷贝"即对拷贝其他终端共享的数据做审计。
- "审计共享目录":共享目录即本机的共享文件夹,共享文件夹中的数据源于本地磁盘。"审计共享目录"即审计其他终端访问本机的共享目录。文件属本地磁盘,可以对共享目录中的数据做操作控制。

注意:注意选择包含子目录,否则审计文件夹下的子目录将无审计。

## 12.2.2 文件操作审计及控制页面



配置介绍



| 配置项:                                   | 说明  |
|--|---|
| 策略名称                                   | 输入合适的策略名称,以方便管理。  |
| 审计目录                                   | 即审计的目录范围,系统默认策略无法更改。  |
| 审计内容                                   | 即对哪些文件操作行为审计。   |
| 操作阻止                                   | 即对哪些文件操作行为阻止, Windows 系统文件拷贝的控制等同于文件读取和写入。                          |
| 文件名关键字                                 | 即文件的后缀名,可以仅审计 doc, txt 等格式。   |
| 进程                                     | 可对指定的进程做判断,例如不审计杀毒软件<br>读取的文件名。                                     |
| 生效时间                                   | 可以选择"所有时间""工作时间""非工作时<br>间""以下时间段"生效,"开始时间"以及"结<br>束时间"仅对"以下时间段"有效。 |
|  | 点击"查看及编辑"超链接,对象类型可以选  |
| 策略应用对象                                 | 择"IP组"、"用户组"、"工作组"、"主机名"  |
| ////////////////////////////////////// | 四种类型,选择相应的应用对象则启用文件操  |
|  | 作审计及控制策略。   |

### 配置要点

1、 点击"添加"文件操作审计及控制策略,如下图:



| and the second second |  |
|-----------------------|--|
| 解释名称                  | 审计"我的文档"                                     |
| 解暗描述                  | -  |
| 审计目录                  | -<br>NUSERPROFILEN 团名子目引                     |
|                       | 支持的研究变量 WrograstilerS, SainderS              |
| 审计内容                  | 团读 团写 团创建 团裁解 团改名/移动 团文件构成                   |
| 操作理止                  | □读 □写 □250 □898 □826 □826/\$60               |
| 文件名关键字                |  |
| 进程                    |  |
| 1991) <b>0</b>        | ●新朝时间 ○工作时间 ○車工作时间 ○以下时间段<br>开始时间 常可时间 增加 時代 |
|                       | 1012-00-10 04000 0012-09-10 10400 5540       |
| 在結構或                  | 图在《理计生效 图 篇《理计生效                             |
| 解释应用对象                | (还没有应用到任何对象) 查查22/指摘                         |

2、点击"策略应用对象"->"查看及编辑"超链接,关联指定的 IP
 组、用户组、工作组、主机名,如下图。选择指定的 IP 组、用户

组、工作组、主机名,并"确定":



3、"保存"并更新客户端规则。

**说明:**系统环境变量均提供支持,打开命令行,输入 set 命令即可查 看所有环境变量,如下图:





# 12.2.3 审计网络拷贝页面

#### 配置要点

4、 点击"添加"文件操作审计及控制策略,如下图:





5、点击"策略应用对象"->"查看及编辑"超链接,关联指定的 IP 组、用户组、工作组、主机名,如下图。选择指定的 IP 组、用户 组、工作组、主机名,并"确定":

| 文件操作审计                | 及控制        |                   |       |        |
|-----------------------|------------|-------------------|-------|--------|
| <b>文件操作</b><br>审计网络拷贝 | 审计及控制      | 9J                |       |        |
| 对象类型                  | IP组 •      | 全部清除              |       |        |
| 对象选择                  | 90         | 110               | 140   | 172-90 |
|                       | 222        | 📝 172. 25. 22. 22 | 99100 | 172-85 |
|                       | 📝 10. 201. | 33                |       |        |
|                       | 确定耳        | 则消                |       |        |

6、"保存"并更新客户端规则。

# 12.4. 打印审计及控制

# 12.3.1 关于打印审计

"打印审计"模块可能会被杀毒软件或防木马软件告警为木马 行为,部署前请确认其可信。

# 12.3.2 打印审计页面

### 配置介绍



| 打印审计及招    | 2制              |                |       |
|-----------|-----------------|----------------|-------|
| 策略名称      |                 |                |       |
| 策略描述      |                 |                |       |
| 是否允许打印    | 0 HB 8 445      |                |       |
| 生效时间      | ●新有封肩 ● 工作封肩    | ○ 非工作时间 ○ 以下时间 | ą     |
|           | 并值时间            | 结束时间           | 编辑 明珠 |
|           |                 |                | 添加    |
| 在线模式      | 図在網社教 図画細胞      | 主动             |       |
| 策略应用对象    | (还没有应用到任何对象)    | 查看加编辑          |       |
| 创建类型      | 全間              |                |       |
| 创建者       | jing            |                |       |
| 注;右边有*号的师 | 目必须输入。<br>保存 取消 |                |       |

| 配置项:   | 说明  |
|--------|---|
| 策略名称   | 输入合适的策略名称,以方便管理。  |
| 是否允许打印 | 如果选择"禁用",则无法打印,无审计记录;<br>如果选择"允许"则对打印行为审计。  |
| 在线模式   | 如果选择"在线时生效",则客户端处于在线状<br>态时生效;如果选择"离线时生效"则客户端<br>处于离线时仍生效。如果不选择,则不生效,<br>如不选择"离线时生效",则客户端离线时不对<br>打印行为审计。 |
| 离线策略   | 即客户端离线时可以选择的动作。如在线时可<br>以审计并控制,离线后可以仅审计不控制。   |
| 策略应用对象 | 点击"查看及编辑"超链接,对象类型可以选择"IP组"、"用户组"、"工作组"、"主机名"四种类型,选择相应的应用对象则启用打印审计策略。                                      |

### 配置要点



1、点击"添加"打印审计策略,如下图:

| 打印甲计及货         | 2.449                              |  |          |
|----------------|------------------------------------|--|----------|
| 策略名称           | 财务室打印审计                            |  |          |
| 策略描述           | 财务堂打印审计策略                          | *  |          |
| 是否允许打印<br>生效时间 | ○禁用 ● 允许<br>● 所有时间 ○ 工作时间 ○ 非      | -<br>1 (111) (11) (11) (11) (11) (11) (11) ( | ł        |
|                | 开始机算机<br>2012/05/10 6400           | 結束时间<br>1915年3月1日日日日<br>1915年3月1日日日日         | SALE MOX |
| 在线種式<br>策略应用对象 | 國在48月生效 國高級對主效<br>(还沒有应用到任何对象) 重叠五 | 2/#10  |          |
| 创建类型           | 全局                                 |  |          |
| 创建奏            | jing                               |  |          |
|                |                                    |  |          |

2、点击"应用策略对象"->"查看及编辑"超链接,关联指定的 IP 组、用户组、工作组、主机名,如下图。选择指定的 IP 组、用户 组、工作组、主机名,并"确定":

| <b>打印审计</b> )<br>财务室打印审计 | 及控制<br>+           |                         |       |                    |
|--------------------------|--------------------|-------------------------|-------|--------------------|
| 对象类型                     | IP组 👻              | 全部清除                    |       |                    |
| 对象选择                     | <b>V</b> 140       | 1722545                 | 99100 | 90                 |
|                          | 172.25.90          | 110                     | 222   | 20                 |
|                          | 🔽 172, 25, 20, 123 | 3 📝 172. 25. 1. 110-210 | 84    | 📝 172. 25. 22. 220 |
|                          | 33                 | 🔽 254. x                | ☑mj主机 | 📝 172. 25. 85      |
|                          | 99206              |                         |       |                    |
|                          | 确定取消               |                         |       |                    |

3、 "保存"并更新客户端规则。

# 12.5. 网站审计及控制

12.4.1 网站审计及控制页面

### 配置介绍



|  | 及控制  |
|--|--|
| 業職名称                                     |  |
| 110日:1                                   |  |
| 2017 B. B. B.                            |  |
| <b>広问!空御</b> ]                           | -<br>  |
|  | D 允许访问会有下列关键字的网站   |
|  | ◎ 禁止访问告有下列关键字的网站   |
| 历时审计                                     | ● 对所有的网站访问进行审计   |
|  | ○ 封网站着称会有下列关键字访问进行审计<br>□ 封闭社会教文会有下列关键字访问进行审计  |
| 美融字列表                                    |  |
|  |  |
|  |  |
|  | · · · · · · · · · · · · · · · · · · ·  |
| NTTP代理                                   |  |
| WIIH CIE                                 | ◎ 允许使用xrrr代理服务器上同以下列表中的代理服务器除外)  |
| arini49≣                                 | ● 允许使用XTTF代理服务器上同以下列表中的代理服务器除外) ● 禁止使用XTTF代理服务器上同以下列表中的代理服务器除外) 04.5年間25年間12月、2015年14月、20158年14月、20158月、20158月、20158月、20158月、20158月、20158月、20158月、20158月、20158月、20158月、20158月、20158月、20158月、20158月、20158月、20158月、20158月、2 |
| un nation                                | ① 计许使用XTTF代理能务器上网以下列表中的代理能务器除外) ② 禁止使用XTTF代理能务器上网(以下列表中的代理能务器除外) 你外代理服务器列表(每行一个,必须是III地址,不能是固名)  |
| and 1                                    | ① 计许使用XTIF代理服务器上网以下列表中的代理服务器除外)<br>② 禁止使用XTIF代理服务器上网以下列表中的代理服务器除外)<br>例外代理服务器列表(每行一个,必须是II地址,不能是成名)。   |
| ain <u>, e</u>                           | <ul> <li>         ① 算止使用xrrf代理服务器上同以下列表中的代理服务器除外)         ② 算止使用xrrf代理服务器上同(以下列表中的代理服务器除外)         例外代理服务器列表(每行一个,必须是III地址,不能是叫名)         。     </li> </ul>  |
| miritige<br>miri编口列表                     | <ul> <li>● 允许使用xttp:代理服务器上同以下列表中的代理服务器除外)</li> <li>● 禁止使用xttp:代理服务器上同以下列表中的代理服务器除外)</li> <li>例外代理服务器列表(每行一个,必须是III地址,不能是成名)</li> <li>●</li> </ul>  |
| m 1145,02<br>m 113编口列表                   | <ul> <li>         ・         ・         ・</li></ul>  |
| 和11時1月<br>和11時間日列表                       | <ul> <li>① 算止使用xrr代理服务器上同以下列表中的代理服务器除外)</li> <li>① 算止使用xrr代理服务器力局以下列表中的代理服务器除外)</li> <li>你外代理服务器列表/每行一个,必须是正地址,不能是成為)</li> <li>。</li> <li>。</li> <li>添加端口</li> </ul>   |
| nt TF 编口列表                               | <ul> <li>● 允许使用xttp代理服务器上同以下列表中的代理服务器除外)</li> <li>● 禁止使用xttp代理服务器为其。(每行一个,必须是非地址,不能是成名)</li> <li>●</li> <li></li></ul>   |
| 和77939<br>和779端口列表<br>审计选项               | <ul> <li>① 算止使用xTT行理服务器上同以下列表中的行理服务器除外)</li> <li>② 算止使用xTT行理服务器力同以下列表中的行理服务器除外)</li> <li>例外气理服务器列表/每行一个,必须是II地址,不能是成為)</li> <li>● 添加端口 不添加的对解有端口生效</li> </ul>  |
| miring<br>mirig口列表<br>車计选项               | <ul> <li>① 禁止使用xtrt代理服务器上网以下列表中的代理服务器除外)</li> <li>① 禁止使用xtrt代理服务器上网以下列表中的代理服务器除外)</li> <li>例外代理服务器列表 每行一个,必须是正地址,不能是成為)</li> <li>● 添加端口</li> <li>● 添加端口</li> <li>● 添加端口</li> <li>● 新计详细的访问日志</li> <li>● 仅审计所访问的资料</li> </ul>   |
| nt TF 编口列表<br>和TF 编口列表<br>审计选项<br>主劲时间   | <ul> <li>● 允许使用xt环代理解务器上同以下列表中的代理服务器除外)</li> <li>● 算止使用xttr代理服务器为其。每行一个,必须是让地址,不能是成名)</li> <li>● 例外代理服务器列表(每行一个,必须是让地址,不能是成名)</li> <li>● 承加限引新有端口主知</li> <li>● 承加限引新有端口主知</li> <li>● 第十译曲的访问日志</li> <li>● 仅审计附访问日志</li> <li>● 仅审计附访问的网站</li> <li>● 新有时间 ● 工作时间 ● 車工作时间 ● 以下时间接</li> </ul>  |
| 和779%(回列表)<br>和779%(回列表)<br>率计选项<br>生效时间 | <ul> <li>● 允许使用xttr代理服务器上网以下列表中的代理服务器除外)</li> <li>● 算止使用xttr代理服务器上网以下列表中的代理服务器除外)</li> <li>● 例外代理服务器列表 每行一个,必须是正地址,不能是成為)</li> <li>● 添加端口</li> <li>● 添加端口</li> <li>● 添加端口</li> <li>● 添加端口</li> <li>● 前十详细的访问日志</li> <li>● 依审计解访问印志</li> <li>● 依审计解访问的知道</li> <li>● 新有时间 ● 工作时间 ● 東工作时间 ● 以下时间段</li> <li>开始时间 ● 東工作时间 ● 以下时间段</li> </ul>  |
| mitriga<br>mitri编口列表<br>單计选项<br>生效时间     | <ul> <li>● 允许使用xtx代理服务器上同以下列表中的代理服务器除外)</li> <li>● 算止使用xtx代理服务器上同以下列表中的代理服务器除外)</li> <li>● 新小节理服务器列表 每行一个。必须是正地址,不能是成為)</li> <li>● 新小节组的访问日志</li> <li>● 原计详细的访问日志</li> <li>● 仅审计解访问印志</li> <li>● 预算计算 ● 算工作时间 ● 以下时间段</li> <li>● 预算计算 ● 算工作时间 ● 以下时间段</li> <li>● 预算计算 ● 算工作时间 ● 以下时间段</li> </ul>   |

| 配置项:     | 说明                              |  |
|----------|---------------------------------|--|
| 策略名称     | 输入合适的策略名称,以方便管理。                |  |
|          | 如果选择"允许访问",则可以访问网络;             |  |
|          | 如果选择"允许访问含有下列关键字的网站",           |  |
| 计自场制     | 则 URL 中含有相关关键字时可以访问, 否则无        |  |
| 「山工」「山工」 | 法访问;如果选择"禁止访问含有下列关键字            |  |
|          | <b>的网站",</b> 则 URL 中含有相关关键字时无法访 |  |
|          | 问, 否则可以访问;                      |  |
| 访问审计     | 如果选择"对所有的网站访问进行审计",则客           |  |

|           | 户端所有 URL 访问均审计;如果选择"对网站                  |
|-----------|--|
|           | 名含有下列关键字访问进行审计"则客户端仅                     |
|           | 审计 URL 中含有关键字表中的网站访问。如果                  |
|           | 选择 "对网站名 <mark>不含有下列关键字访问进行</mark> 审     |
|           | 计"则客户端仅审计 URL 中含有关键字表外的                  |
|           | 其他任何网站访问。                                |
|           | 即URL中含有的字符串,例如:                          |
| 关键字列表     | http://www.baidu.com, 中的".bai"、"idu.co"、 |
|           | "baidu"等等。不审计 html 中的关键字内容。              |
|           | 如果选择"允许使用 HTTP 代理服务器上网(以                 |
|           | <b>下列表中的代理服务器除外)</b> ",则将禁止使用            |
| иттр 伊珊   | 列表中的代理名称或 IP 地址;如果选择"禁止                  |
| ni ir 心理  | 使用 HTTP 代理服务器上网(以下列表中的代                  |
|           | 理服务器除外)",则仅允许使用列表中的代理                    |
|           | 名称或 IP 地址。                               |
|           | 如果不输入则默认对所有端口的 HTTP 访问均                  |
| HTTP 端口列表 | 审计,如果添加了 80 端口,则仅审计 80 端口                |
|           | 的 HTTP 网站访问。                             |
|           | "审计详细的访问日志"能审计到详细的网站                     |
|           | 访问信息,包括自己访问的网站信息及之后自                     |
|           | 动访问的网站访问行为;                              |
| 审计选项      | "仅审计所访问的网站"仅审计用户实际访问                     |
|           | 的网站,而对一些网站后台自动连接的网站访                     |
|           | 问行为不审计;并且审计周期默认为10分钟,                    |
|           | 即十分钟内的重复数据不上报                            |
|           | 可以选择"所有时间""工作时间""非工作时                    |
|           |  |
| 生效时间      | 间""以下时间段"生效,"开始时间"以及"结                   |



|        | 如果选择"在线时生效",则客户端处于在线状    |
|--------|--------------------------|
|        | 态时生效;如果选择"离线时生效"则客户端     |
| 在线模式   | 处于离线时仍生效。如果不选择,则不生效,     |
|        | 如不选择"离线时生效",则客户端离线时不对    |
|        | 上网行为审计。                  |
|        | 点击"查看及编辑"超链接,对象类型可以选     |
| 等败应用对角 | 择"IP组"、"用户组"、"工作组"、"主机名" |
| 東哈应用刈家 | 四种类型,选择相应的应用对象则启用网站审     |
|        | 计及控制策略。                  |
|        |                          |

### 配置要点

1、 点击"添加"网站访问控制与审计。

| 策略名称                                  | 公司员工网络审计 *  |     |
|---------------------------------------|---|-----|
| 策略描述                                  | *   |     |
|                                       | *   |     |
| 访问控制                                  | ◎ 允许访问  |     |
|                                       | ◎ 允许访问含有下列关键字的网站  |     |
|                                       | ◎ 禁止访问含有下列关键字的网站  |     |
| 历问审计                                  | 到所有的网站访问进行审计  |     |
|                                       | ◎ 对网站名称含有下列关键字访问进行审计  |     |
| · · · · · · · · · · · · · · · · · · · | ◎ 对网站名称不含有下列关键字访问进行审计   |     |
| 大键子列表                                 | *   |     |
|                                       |   |     |
|                                       | —————————————————————————————————————                             |     |
| HTTP代理                                | ◎ 允许使用HTTP代理服务器上网(以下列表中的代理服务器除                                    | 外)  |
|                                       | ◎ 禁止使用)ITTP代理服务器上网(以下列表中的代理服务器除<br>例外代理服务器列表(每行一个,必须是IP地址,不能是域名): | ቃՒ) |
|                                       | *   |     |

2、 点击策略应用对象的"查看及编辑"超链接,选择指定的 IP

组、用户组、工作组、主机名,则这些 IP 组、用户组、工作组、

主机名中的电脑启用上网审计或控制策略。

| <b>网站访问审</b><br>公司员工网络审词 | '计及控制<br>⁺         |                       |       |                  |
|--------------------------|--------------------|-----------------------|-------|------------------|
| 对象类型                     | IP组 ▼ 全            | 部清除                   |       |                  |
| 对象选择                     | <b>V</b> 140       | ☑ 1722545             | 99100 | 90               |
|                          | 📝 172. 25. 90      | <b>V</b> 110          | 222   | 20               |
|                          | ☑ 172. 25. 20. 123 | ☑ 172. 25. 1. 110-210 | 📝 84  | 172. 25. 22. 220 |
|                          | 33                 | <b>V</b> 254. x       | ☑mj主机 | 📝 172. 25. 85    |
|                          | 99206              |                       |       |                  |
|                          | 确定取消               |                       |       |                  |

3、 "保存"并更新客户端规则。

# 12.6. FTP 审计及控制

# 12.5.1 FTP 审计及控制页面

### 配置介绍





| 配置项: | 说明                                 |  |
|------|------------------------------------|--|
| 策略名称 | 输入合适的策略名称,以方便管理。                   |  |
|      | 如果选择"允许 FTP 访问",则可以访问所有            |  |
|      | FTP 服务器;如果选择"允许访问含有下列地             |  |
|      | <b>址的 FTP 服务器"</b> ,则仅 FTP 地址中含有关键 |  |
| 访问控制 | 字表中的服务器可以访问,否则无法访问;如               |  |
|      | 果选择"禁止访问含有下列地址的 FTP 服务             |  |
|      | 器",则 FTP 地址中含有关键字表中的服务器            |  |
|      | 无法访问, 否则可以访问;                      |  |
|      | 如果选择"对所有的 FTP 访问进行审计",则            |  |
| 法同审计 | 客户端所有 FTP 访问均审计;如果选择"对下            |  |
| 可可可  | <b>列地址中的 FTP 服务器访问进行审计"</b> 则客户    |  |
|      | 端仅审计 FTP 地址中含有关键字表中的 FTP 访         |  |



|           | 问。如果选择"对不在下列地址中的 FTP 服务  |
|-----------|--|
|           | 器访问进行审计"则客户端仅审计 FTP 地址中  |
|           | 含有关键字表外的其他任何 FTP 访问。   |
|           | 即 FTP 服务器中的 IP 地址,如: 10.201.1.202;   |
| FTP 服务器列表 | 如果不输入则默认对所有的 FTP 访问控制并审  |
|           | 计。   |
|           | 如果不输入则默认对所有端口的 FTP 访问均控  |
| FTP 端口列表  | 制并审计,如果添加了21端口,则仅控制并审  |
|           | 计 21 端口的 FTP 访问。   |
|           | 可以选择"所有时间""工作时间""非工作时  |
| 生效时间      | <b>问""凹下时间的"</b> 开始" <b>工始时间"</b> 凹及" <b>佐</b>   |
| 工業時間      | 问 以下时间段 主效,开始时间 以及 结   |
| 工 次时 [14] | <b>束时间"</b> 仅对"以下时间段"有效。   |
|           | <b>束时间"</b> 仅对" <b>以下时间段"</b> 有效。<br>如果选择"在线时生效",则客户端处于在线状   |
|           | <b>東时间"</b> 仅对" <b>以下时间段</b> "有效。<br>如果选择"在线时生效",则客户端处于在线状态时生效;如果选择"离线时生效"则客户端   |
| 在线模式      | <b>東时间"</b> 仅对" <b>以下时间段</b> "有效。<br>如果选择"在线时生效",则客户端处于在线状态时生效;如果选择"离线时生效"则客户端处于离线时仍生效。如果不选择,则不生效,   |
| 在线模式      | <b>東时间"</b> 仅对" <b>以下时间段</b> "有效。<br>如果选择"在线时生效",则客户端处于在线状态时生效;如果选择"离线时生效"则客户端处于离线时仍生效。如果不选择,则不生效,如不选择"离线时生效",则客户端离线时不对  |
| 在线模式      | <b>東时间"</b> 仅对" <b>以下时间段</b> "有效。<br>如果选择"在线时生效",则客户端处于在线状态时生效;如果选择"离线时生效"则客户端处于离线时仍生效。如果不选择,则不生效,如不选择"离线时生效",则客户端离线时不对<br>FTP 访问行为审计。   |
| 在线模式      | <ul> <li>南 仅下时间段 主效, 开始时间 以及 第</li> <li>束时间"仅对"以下时间段"有效。</li> <li>如果选择"在线时生效",则客户端处于在线状态时生效;如果选择"离线时生效"则客户端处于离线时仍生效。如果不选择,则不生效,如不选择"离线时生效",则客户端离线时不对</li> <li>FTP 访问行为审计。</li> <li>点击"查看及编辑"超链接,对象类型可以选</li> </ul>   |
| 在线模式      | <ul> <li>内 以下时间段 主效, 开始时间 以及 第</li> <li>束时间" 仅对"以下时间段"有效。</li> <li>如果选择"在线时生效",则客户端处于在线状态时生效; 如果选择"离线时生效"则客户端处于离线时仍生效。如果不选择,则不生效,如不选择"离线时生效",则客户端离线时不对</li> <li>FTP 访问行为审计。</li> <li>点击"查看及编辑"超链接,对象类型可以选择"IP 组"、"用户组"、"工作组"、"主机名"</li> </ul>                                |
| 在线模式      | <ul> <li>内 以下时间段 主效, 开始时间 以及 第</li> <li>束时间"仅对"以下时间段"有效。</li> <li>如果选择"在线时生效",则客户端处于在线状态时生效;如果选择"离线时生效"则客户端处于离线时仍生效。如果不选择,则不生效,如不选择"离线时生效",则客户端离线时不对</li> <li>FTP 访问行为审计。</li> <li>点击"查看及编辑"超链接,对象类型可以选择"IP 组"、"用户组"、"工作组"、"主机名"</li> <li>四种类型,选择相应的应用对象则启用 FTP 审</li> </ul> |

### 配置要点

1、点击"添加""FTP访问审计及控制"



| 兼略名称                                  | FTP访问审计及控制                                | *              |
|---------------------------------------|---|----------------|
| 策略描述                                  |   | *              |
| 访问控制                                  |   |                |
| , , , , , , , , , , , , , , , , , , , | ● 允许FTP访问                                 |                |
|                                       | ◎ 允许访问含有下列地址的FTP服务器                       |                |
| ر ، بسرد ب                            | ◎ 禁止访问含有下列地址的FTP服务器                       |                |
| 加回申计                                  | ◎ 对所有的PTP访问进行审计                           |                |
|                                       | ◎ 对下列地址中的FTP服务器访问进行                       | 审计             |
|                                       | ◎ 对不在下列地址中的FTP服务器访问                       | 进行审计           |
| TP服务器列表                               |   | +              |
|                                       |   |                |
|                                       |   |                |
|                                       |   | >>             |
| TP端口列表                                |   | +              |
|                                       |   |                |
|                                       |   |                |
|                                       |   | >>>            |
| 效时间                                   | ◙ 所有时间 ◎ 工作时间 ◎ 非工作时                      | 间 🔍 以下时间段      |
|                                       | 开始时间                                      | 结束时间 编辑 删除     |
|                                       | 2012-03-10 9:00 2012-                     | 03-10 13:30 添加 |
|                                       |   |                |
| E线模式                                  | 7 方线相开动 7 南线相升开动                          |                |
|                                       | 1 1 1 2 3 H V T X 2 1 1 1 2 3 3 H V T X 2 |                |

- 2、点击策略应用对象的"查看及编辑"超链接,选择指定的 IP 组、用户组、工作组、主机名,则这些 IP 组、用户组、工作组、主机名中的电脑启用 FTP 审计及控制策略。
- 4、"保存"并更新客户端规则。

# 12.7. 文件涉密信息审计

## 12.6.1 文件涉密信息审计页面

### 配置介绍




| 配置项:      | 说明  |
|-----------|---|
| 策略名称      | 输入合适的策略名称,以方便管理。  |
| 关键字列表     | 可增加一个或者多个关键字,如果文件内容中<br>包含该关键字,则将被审计出来                              |
| 关键字之间关系   | 有'与'和'或'两种。'与'则审计包含所有<br>的关键字,'或'则审计包含任意关键字                         |
| 仅审计一下文档类型 | 可对需要审计的文档类型进行筛选。如".txt"   |
| 生效时间      | 可以选择"所有时间""工作时间""非工作时<br>间""以下时间段"生效,"开始时间"以及"结<br>束时间"仅对"以下时间段"有效。 |
| 在线模式      | 如果选择"在线时生效",则客户端处于在线状<br>态时生效;如果选择"离线时生效"则客户端                       |



|        | 处于离线时仍生效。如果不选择,则不生效,     |
|--------|--------------------------|
|        | 如:不选择"离线时生效",则客户端离线时不    |
|        | 对涉密文档进行审计。               |
|        | 点击"查看及编辑"超链接,对象类型可以选     |
| 策略应用对象 | 择"IP组"、"用户组"、"工作组"、"主机名" |
|        | 四种类型,选择相应的应用对象则启用文件涉     |
|        | 密信息审计策略。                 |

#### 说明

- 文件涉密信息审计是对文件内容进行审计,而不是文件名。
- 要使得此策略生效,必须要确保开启终端上的 Windows Search 服务。Windows 7 默认就有该服务,只需确保该服务已启动就可以;
   但 Windows 7 之前的系统都是默认没有 Windows Search 服务的,必须安装 KB940157 补丁,然后确保启动了 Windows Search 服务。
- 确保 Windows Search 服务启动后,还需要手动为需要审计的位置
   建立索引,不同系统建立索引的方法见 附录1
- KB940157 下载链接参考:
   <a href="http://www.microsoft.com/windows/products/winfamily/des">http://www.microsoft.com/windows/products/winfamily/des</a>
   <a href="http://ktopsearch/choose/windowssearch4.mspx?tab=Install%20It">http://www.microsoft.com/windows/products/winfamily/des</a>
   <a href="http://ktopsearch/choose/windowssearch4.mspx?tab=Install%20It">http://www.microsoft.com/windows/products/winfamily/des</a>
- 文件涉密信息审计不支持 windows 2000。
- 文件涉密审计能审计的文档类型与 windows search 支持的类型一 致,如:.txt.ini.jpg.cpp.xls.cc.cpp.log.xml Office 文档 电子邮件等。
- 文件涉密信息审计策略与升级策略存在冲突,管理员可以自行处理 避免两种策略同时出现。

#### 配置要点



1、单击"添加" 文件涉密信息审计策略

| ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ |                                   |                     |    |
|--|-----------------------------------|---------------------|----|
| 又忤涉密信息审                                | ार्म                              |                     |    |
| 策略名称                                   | 文件涉密信息审计                          | *                   |    |
| 策略描述                                   |                                   | *                   |    |
|  |                                   | +                   |    |
| 关键字列表                                  | ad                                | .*                  |    |
|  |                                   | <b>*</b>            |    |
|  | 每个关键字一行,可以输入多个关键。<br>审计句令任意关键字的文档 | ≩                   |    |
| 关键字之间的关系                               |                                   |                     |    |
| 仅审计以下文档类型                              |                                   | <b>↓</b> g∏:". txt" |    |
|  |                                   |                     |    |
|  |                                   | * >>                |    |
| 生效时间                                   | ◎ 所有时间 🔘 工作时间 🔘 非工作               | 作时间 🔘 以下时间段         |    |
|  | 开始时间                              | 结束时间 编辑 🛚           | 刚除 |
|  | 2012-03-10 9:00 201               | 2-03-10 13:30 添加    |    |
| 在线模式                                   | ☑ 在线时生效 ☑ 离线时生效                   |                     |    |
| 策略应用对象                                 | (还没有应用到任何对象) 查看及编                 | <u>辑</u>            |    |
| 创建类型                                   | 全局                                |                     |    |
| 创建者                                    | jing                              |                     |    |
| 注: 右边有*号的项目必                           | ·须输入。                             |                     |    |
|  | 保存取消                              |                     |    |

2、点击策略应用对象的"查看及编辑"超链接,选择指定的 IP 组、用户组、工作组、主机名,则这些 IP 组、用户组、工作组、主机名中的电脑启用文件涉密信息审计策略。

"保存"并更新客户端规则。

### 12.6.2 附录1

不同的操作系统在安装完**补丁 KB940157** (windows 7 不需要安装此补丁)后,需 要手动给需要审计的位置添加索引,如下:

#### Windows 2003

安装补丁 KB940157 后,确定 Windows Search 服务启动后,点击 "开始一》
 控制面板一》Indexing Options"出现如下页面:



| dering Option   | 5                                  |  |
|---|------------------------------------|--|
| 218<br>Ind  | ) items indexed<br>exing complete, |  |
| ndex these location<br>Included Locations<br>李本地磁盘 (C:) | S:                                 | Exclude<br>Application Data; Default User; Program Fil |
|   |                                    |  |
|   |                                    |  |
|   |                                    |  |
| Modify  | Advanced                           |  |
|   |                                    | Close  |

2、单击 "Modify", 然后勾选你需要添加索引的位置。 然后点击"确定"

#### Windows XP

 安装补丁 KB940157 后,确定 Windows Search 服务启动后,"开始一》控制 面板一》性能和维护一》Indexing Options",然后出现如下页面:

| dexing Opt     | ions                    |          |         |
|----------------|-------------------------|----------|---------|
| 2              | 218 items<br>Indexing ( | indexed  |         |
| ndex these loc | ations:<br>tions        |          | Exclude |
|                |                         |          |         |
| Modify         | 1                       | Advanced |         |
| Modify         |                         | Agvanced |         |
|                |                         |          | Close   |

2、单击 "Modify", 然后勾选你需要添加索引的位置。 然后点击"确定"

#### Windows 2008

1、安装补丁 KB940157 后,确定 Windows Search 服务启动后。"开始一》控制



| 已为 297 项键             |                      |  |
|-----------------------|----------------------|--|
| 日子用户活动                | ▶ 案5旧刘 <b>巫</b> 厦减慢。 |  |
| 下列位署建立委引・             |                      |  |
| 123位血星亚东 11.<br>可含的位置 | 排除                   |  |
| 「开始」菜单                | 120020121            |  |
| ■ 用戸                  | Default              |  |
|                       |                      |  |
|                       |                      |  |
|                       |                      |  |
|                       |                      |  |
|                       |                      |  |
|                       |                      |  |
| (修改 (M) 🔰 🕼           | )高级 (0) 📔 🕐 暫停 (P) 丨 |  |
|                       |                      |  |

面板一》索引选项",点击进入到以下页面:

2、单击上图中的"修改"为你所需要的位置建立索引。

#### Windows Vista

1、安装补丁 KB940157 后,确定 Windows Search 服务启动后。"开始一》控制 面板一》系统和维护一》索引选项"点击 如下图:





| a) 案引选项  |                  |
|--|------------------|
| 已为 162 项建立索引<br>由于用户活动,索引的速度和<br>为下列位置建立案引:      | 劇∰ ∘             |
| 包含的位置  | 利服余              |
| → 「开始」菜単<br>→ 用户<br>登 脱机文件(JIAN-VISTAX32\Adminin | Default          |
| [ 修改 00) ] [ 慶高級 00) ]<br>索引如[個景調局授家 00)2        | [ ● 暂停 (P) ]<br> |

2、单击上图中的"修改"为你所需要的位置建立索引。

#### Windows 7

 确定 Windows Search 服务启动后。点击"开始—》控制面板",然后将查看 方式改为"小图标",单击"索引选项"如下图:

|  |                        | ▼ 41 ##E4.2#                           |  |
|--|------------------------|--|--|
| 调整计算机83设置                                |                        |  |  |
| Flittocker Bittettal                     | C Internet 50          | P ODEC                                 |  |
| RemoteApp 和國際語語                          | 🗃 Windows CandSpace    | Mil Windows Defender                   |  |
| Windows Update                           | Windows In A M         | Windows #30++()                        |  |
| * 常白和正用                                  | OFFIR T                | 國程序和功能                                 |  |
| 日本 日 | <b>建</b> 用用点式          | ₩ 个性化                                  |  |
| <b>具工新教</b>                              | 4 <sup>29</sup> (75.81 | *3 # XM                                |  |
| 2 特点:                                    | の世に指示                  | ₩ 決諾爾德維                                |  |
| 2 轻相动将中心                                 | Թ (Exceloration        | 4. 任務性和「开始」 三章                         |  |
| 2 白柳的拉根                                  | ALC IN                 | A ···································· |  |
| 自治無和行助性                                  | 4 <b>A</b> H           | ♪ 翻标                                   |  |
| 2. 索引建筑                                  | III 進和IE #图例           | () 局步中心                                |  |
| ■ 料槽和外菜田()                               | 期 位置和其他地等群             | 文件实送稿                                  |  |
| ● 新研                                     | <b>要</b> 重示:           | ■ 性紙俱密和工具                              |  |
| 3 股份推进                                   | 1. 美国市大学               | 起 而户能户                                 |  |
| 3 mit                                    | 0 mm/281               | 副 桌用小工具                                |  |
| 「日本語は                                    | 1 = a                  |  |  |



| 已为 102,056 项建立索引<br>条引完成。  |                                       |
|--|---------------------------------------|
| 为这些位置建立索引:<br>————————————————————————————————————   | 排除                                    |
| <ul> <li>「开始」菜单</li> <li>Document (F:)</li> <li>Download (G:)</li> <li>Internet Explorer 历史记录</li> <li>Internet ficture</li> <li>wirdows 便笺 (jian99-PC\Adminis</li> <li>Windows7 (C:)</li> <li>Windox</li> </ul> | ProgramData; Data; AppData; AppDa     |
| * · · · · · · · · · · · · · · · · · · ·  | · · · · · · · · · · · · · · · · · · · |

2、单击上图中的"修改"为你所需要的位置建立索引。

## 12.8. 应用程序使用审计

### 12.7.1 应用程序使用审计页面

配置介绍

#### 应用程序使用审计 策略名称 审计进程 策略描述 审计进程 . 审计行为 ◉ 审计指定进程 ◎ 审计所有进程 进程列表 ¥ cmd. exe notepad.exe taskmgr.exe mspaint.exe >> 生效时间 ◉ 所有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段 开始时间 结束时间 编辑 添加 在线模式 🔽 在线时生效 📝 离线时生效 策略应用对象 (还没有应用到任何对象) 查看及编辑 创建类型 全局 创建者 jing 注: 右边有\*号的项目必须输入。 保存 取消



| 配置项:   | 说明   |
|--------|--|
| 策略名称   | 输入合适的策略名称,以方便管理。   |
| 审计行为   | 可以选择是对所有程序进行审计,还是对指定<br>的几个进程进行审计;如果选择"审计指定进<br>程"则由管理员自己确定进程名列表,如果选<br>择"审计所有进程"则任务管理器中的进程列<br>表里面进程全部可以审计出来  |
| 进程列表   | 只有当审计行为选择为"审计指定进程",这<br>里才会变为可编写,可以添加一个或多个进程<br>名  |
| 生效时间   | 可以选择"所有时间""工作时间""非工作时<br>间""以下时间段"生效,"开始时间"以及"结<br>束时间"仅对"以下时间段"有效。  |
| 在线模式   | 如果选择"在线时生效",则只对客户端处于在<br>线状态时的进程运行情况进行审计;如果选择<br>"离线时生效"则只对客户端处于离线状态时<br>的进程运行情况进行审计。如果不选择,则不<br>生效,如:只选择"在线时生效",则只审计客<br>户端在线时的进程运行情况,而不审计离线状<br>态下的进程运行情况。 |
| 策略应用对象 | 点击"查看及编辑"超链接,对象类型可以选择"IP组"、"用户组"、"工作组"、"主机名"四种类型,选择相应的应用对象则启用应用程序使用审计策略。   |

**说明**:应用程序审计会将程序创建时间、退出时间和连续运行时间审 计下来,且只有当程序结束才会上报运行情况,未结束的程序运行情 况不立即上报,只记载在客户端。



1、点击"添加"应用程序使用审计策略

|                        | 审计进程  | *                                   |       |
|------------------------|---|-------------------------------------|-------|
| 策略描述                   | 审计进程  | *                                   |       |
| 审计行为                   | <ul> <li>审计指定进程</li> </ul>  | +所有进程                               |       |
| 进程列表                   |   |                                     |       |
| 生效时间                   | cmd.exe<br>notepad.exe<br>taskmgr.exe<br>mspaint.exe<br>● 所有时间 ① 工作时间 ① 非 | >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>> |       |
|                        | 开始时间  | 结束时间                                | 编辑 删除 |
|                        | 2012-03-10 9:00   | 2012-03-10 13:30                    | 添加    |
|                        |   |                                     |       |
| 在线模式                   | 🗹 在线时生效 🗹 离线时生效   |                                     |       |
| 在线模式<br>策略应用对象         | ☑ 在线时生效 ☑ 离线时生效<br>(还没有应用到任何对象) 查看  | 及编辑                                 |       |
| 在线模式<br>策略应用对象<br>创建类型 | ▼在线时生效 ▼离线射生效<br>(还没有应用到任何对象) 查看<br>全局                                    | 及编辑                                 |       |

- 点击策略应用对象的"查看及编辑"超链接,选择指定的 IP 组、用户 组、工作组、主机名,则这些 IP 组、用户组、工作组、主机名中的电脑启 用应用程序使用审计策略。
- 3、 "保存"并更新客户端规则。

## 12.9. 刻录审计

### 12.8.1 刻录审计策略页面



| 刻录审计     |  |                            |
|----------|--|----------------------------|
| 策略名称     | 刻录审计   | *                          |
| 策略描述     | 刻录审计   | *                          |
| 审计选项     | <ul> <li>允许刻录,不审计刻录文件</li> <li>允许刻录,审计刻录文件</li> </ul>  |                            |
| 生效时间     | <ul> <li>○ 禁用刻录</li> <li>● 所有时间 ○ 工作时间 ○ 非工作时间 ○ 以下時</li> <li>● 开始时间</li> <li>● 2012-03-10 9:00</li> <li>2012-03-10 13:30</li> </ul> | <b>捕殺</b><br>编辑 删除<br>了 添加 |
| 在线模式     | ☑ 在线时生效 ☑ 离线时生效  |                            |
| 策略应用对象   | (还没有应用到任何对象) 查看及编辑   |                            |
| 创建类型     | 全局   |                            |
| 创建者      | jing   |                            |
| 注:右边有*号的 | 的项目必须输入。   |                            |

| 策略名称   | 输入合适的策略名称,以方便管理。                  |
|--------|-----------------------------------|
|        | "允许刻录,不审计刻录文件",允许终端刻录             |
|        | 且不会审计终端的刻录行为;                     |
| 审计选项   | "允许刻录,审计刻录文件",允许终端刻录且             |
|        | 终端刻录的动作将会被审计;                     |
|        | "禁止刻录",禁止终端的刻录行为                  |
|        | 可以选择"所有时间""工作时间""非工作时             |
| 生效时间   | 间""以下时间段" 生效, "开始时间" 以及"结         |
|        | <b>束时间"</b> 仅对" <b>以下时间段"</b> 有效。 |
|        | 如果选择"在线时生效",则只对客户端处于在             |
|        | 线状态时刻录行为进行控制和审计;如果选择              |
| 在线模式   | "离线时生效"则只对客户端处于离线状态时              |
|        | 的刻录行为进行控制和审计。如果不选择,则              |
|        | 不生效                               |
| 策略应用对象 | 点击"查看及编辑"超链接,对象类型可以选              |



| 择"IP组"、"用户组"、"工作组"、"主机名" |
|--------------------------|
| 四种类型,选择相应的应用对象则启用刻录审     |
| 计策略。                     |

#### 说明

- 刻录审计只能审计到利用 windows 自带的刻录功能进行的审计,
   第三方软件的刻录行为审计不到
- 禁止刻录除了可以禁止 windows 自带的刻录以外,还可以禁止:
   UltraISO、Magic ISO Maker、IsoBuster、ImgBurn

#### 配置要点

1、点击"添加"刻录审计策略

| 刻录审计   |  |
|--------|--|
| 策略名称   | 刻录审计 *   |
| 策略描述   | 刻录审计   |
| 审计选项   | <ul> <li>● 允许刻录,不审计刻录文件</li> <li>● 允许刻录,审计刻录文件</li> <li>● 允许刻录,审计刻录文件</li> </ul> |
| 生效时间   | ◎ 新有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段<br>开始时间  |
| 在线模式   | 🗹 在绑时生效 🗹 离绑时生效  |
| 策略应用对象 | (还没有应用到任何对象) 查看及编辑   |
| 创建类型   | 全局   |
| 创建者    | jing   |
|        |  |

- 2、 点击策略应用对象的"查看及编辑"超链接,选择指定的 IP 组、用户 组、工作组、主机名,则这些 IP 组、用户组、工作组、主机名中的电脑启 用刻录审计。
- 3、 "保存"并更新客户端规则。



# **12.10.** Windows 事件日志审计

### 12.9.1Windows 事件日志审计页面

#### 配置介绍 Windows事件日志审计 Windows事件日志审计 策略名称 Windows事件日志审计 策略描述 \* 🗵 发送应用程序日志到服务器 ☑发送安全日志到服务器 ☑ 发送系统日志到服务器 生效时间 ◎ 所有时间 ◎ 工作时间 ◎ 非工作时间 ◎ 以下时间段 开始时间 结束时间 编辑 删除 添加 在线模式 ☑在线时生效 ☑离线时生效 策略应用对象 (还没有应用到任何对象) 查看及编辑 创建类型 全局 创建者 jing 注: 右边有\*号的项目必须输入。 取消 保存

| 策略名称        | 输入合适的策略名称,以方便管理。                  |
|-------------|-----------------------------------|
|             | 输入适当的描述,以方便管理。选择 <b>"发送应</b>      |
| 笙吹描述        | 用程序日志到服务器"或"发送安全日志到服              |
| 東哈迪处        | <b>务器" 或 "发送系统日志到服务器"</b> ,客户端将   |
|             | 会把相应的日志上报给服务器。                    |
|             | 可以选择"所有时间""工作时间""非工作时             |
| 生效时间        | 间""以下时间段" 生效, "开始时间" 以及"结         |
|             | <b>束时间"</b> 仅对" <b>以下时间段"</b> 有效。 |
| <b>左</b> /{ | 对于 Windows 事件日志审计,在线模式功能无         |
| 任线保入        | 效                                 |



|  | 点击"查看及编辑"超链接,对象类型可以选     |
|--|--------------------------|
| 签收应用对角   | 择"IP组"、"用户组"、"工作组"、"主机名" |
| <b></b> <sup><sup><sup>1</sup></sup> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup></sup></sup> | 四种类型,选择相应的应用对象则启用        |
|  | Windows 事件日志审计策略。        |

## 13. 桌面运维

## 13.1. 关于桌面运维

天珣除了提供资产管理、远程桌面、软件分发等通用的终端运维管理功能 模块之外,还提供了多种桌面运维工具,例如主机名规范、企业短消息、终端资 源监控、Windows防火墙例外、终端实时操控等,为管理员提供高效工具,成为 管理员终端运维的好帮手。



# 13.2. 软件分发

### 13.2.1. 关于软件分发

■ 软件分发在天珣产品功能模块中属于相对比较独立一个功能,



其主要用于对受控终端进行统一的软件或者文件的分发。

- 软件分发不仅能对可执行文件 exe,标准 msi 等安装程序进行 分发,也能直接下发文件或文件夹,并可针对判断条件进行设置,便于对执行过程中的任何问题进行监控。
- 软件分发可以支持域环境下普通用户帐户对分发的软件进行 安装。

### 13.2.2. 软件分发设置页面

#### 配置介绍

| 教件分发           | 教件分发查询  | 教育分3     | (数认参数    |          |      |            |     |      |
|----------------|---------|----------|----------|----------|------|------------|-----|------|
| 软件分发           | at its  |          |          |          |      |            |     |      |
| 非自治用           | 北齐属派    | 我发生      | 巴克成      | 分生人业     | 兵充状条 | 化合新止日期     | 推荐  | - 10 |
| test           |         | 11       | 1        | 1        | 拉邦过程 | 2012-10-17 | +   |      |
| test_20        | test_20 | 2        | 2        | 2        | 正常   | 2012-10-24 | * * |      |
| <u>idfarfd</u> |         | Ð        | <u>.</u> | 0        | 校验失敏 | 2012-10-24 | * * |      |
| 老林秋            |         | <u>0</u> | 2        | <u>g</u> | 校验失败 | 2012-10-29 | * * |      |
| forts          |         | <u>0</u> | 1        | 2        | 正常   | 2012-10-29 | * * |      |
| tert           |         | 0        | 1        | ġ.       | 正常   | 2012-10-29 | +   |      |
| 1              |         |          |          |          |      |            |     |      |

点击"添加"按钮设置软件分发策略





| IT XX III IX II         | 分发查询 软件分发跟认整数  |
|-------------------------|--|
| 软件分发                    |  |
| 任务条称                    |  |
| 任务新进                    |  |
|                         |  |
|                         |  |
| 15#M                    |  |
| 1000                    | <b>安装包分</b> 版 •  |
| DRXHRXH <del>A</del>    | <u>选择</u> -  |
| 的装包局站程序                 | 选择   |
| 在装塑数                    |  |
| 自标解证                    |  |
|                         | 支持的轩辕变量:%ProgramFiles%,%windir%  |
| 使装造项                    | 三安装箱提示用户   |
|                         | 回以系统用户身份运行   |
|                         | 口该任料不需要与用户交互   |
|                         | 巴克威任务系 分钟关机  |
|                         | []任务失航也执行自动关机  |
| 1分数止日期                  | 10/30/2012 🔤 -   |
| 任务执行时间段                 | 开始时间 结束时间 铜矾 网络  |
|                         |  |
| 201-12-120              | (375-575)(274-5) 75 (199)  |
| 1990年1月1日<br>第三日本の下生分生さ | (TERMONITING) NUCLEAR  |
| Nindows 2000            | No. of Concession, State of Co |
| the dame with           | 12.32m   |
| Aundows XP              | 图 32位 图 64位  |
| Nindows 2003            | 12 32m 12 64m  |
| Mindows Vista           | IV 30位 [] 64位  |
| Nindows 2008            | 图 32位 图 64位  |
| Nindows 7               | 12 32位 12 64位  |
| STATES                  | 25   |
| (建会                     | jing   |
| 满足铁下条件执行                | 安葉   |
| 新经检察                    | ●素字检查 ○检查知径 ○检查注册表 ○检查指径均注册表 ○检查指径均注册表   |
| =####                   | 支持的还属变量: %ProgramFiles%, %windir%  |
| 10.0                    |  |
| 11日赤白湖                  |  |
| -                       | 1419 11489 小丁 八丁 小丁<br>県第子 大王県第子   |
|                         | 24   |
| FALS PARTIES            | ● 都不检索 ○ 检索路径 ○ 检索主要素 ○ 检索路径向注意表 ○ 检索路径或注意表  |
| 新發性質                    | <b>市在 不存在</b>  |
| +max                    | 支持的环境变量: %ProgramFiles%, %windin%  |
| 2018/99<br>注意来落         | 一 存在 一 不存在   |
| 10.00.00.00             | (存在)不存在  |
| THE SOLD                | ○ 相称 ○ 不相称 ○ 小子 ○ 小子   |

| 配置项:     | 说明   |
|----------|--|
| 任务名称     | 为软件分发的任务命名。                                    |
| 任务描述     | 用以描述该任务的详细信息。                                  |
| 任务类型     | 定义分发的文件是何种类型,包括"安装包分<br>发"、"文件分发"和"注册表文件分发"三种。 |
| 分发文件或文件夹 | 选择此次分发的文件所在的路径,点击"选择"                          |

Π



|            | 按钮进行选择。   |
|------------|---|
| 安装包启动程序    | 选择分发的安装包启动时调用的安装文件,仅<br>"安装包分发"时可用。   |
| 安装参数       | 对安装的程序包进行参数设置(当需要设置时<br>可参考安装程序的帮助手册了解其特定的安装<br>参数),仅"安装包分发"时可用。  |
| 目标路径       | 设置被分发的文件将被保存在客户端的哪个路<br>径下面,仅" <b>文件分发"</b> 时可用。注册表文件<br>分发默认路径为C盘,不需要填写目标路径。   |
| 安装选项       | 选项"安装前提示用户"对于软件分发策略下发<br>后在客户端进行提示等待还是执行安装。<br>选项"以系统身份运行",支持域环境下以普通<br>用户帐号对分发的软件进行安装。<br>选项"该任务不需要用户交互"为安装过程不需<br>要用户确认或点"下一步",后台完全静默安装。<br>选项"完成任务后 分钟关机"支持任务完成<br>后自动关机,增加一个可倒计时关机的参数,<br>可选择 1-999 的参数值,一分钟为单位。<br>选项"任务执行失败也自动关机"勾选了完成<br>任务后自动关机,才允许勾选"任务失败也执<br>行自动关机"。 |
| 任务截止日期     | 此软件分发任务最终失效时间,默认为当前日<br>期7天以后,即默认任务有效期为7天。  |
| 任务执行时间段    | 设置此软件分发任务在一天内哪个时间段执行  |
| 策略应用对象     | 关联到 IP 组、工作组、主机名使策略生效   |
| 是否在以下平台生效  | 选择策略生效对应的客户端操作系统平台  |
| 满足以下条件执行安装 | 检查路径或注册表的信息来定义是否让客户端  |



|            | 执行此次的软件分发策略          |
|------------|----------------------|
| 进口以下发供任务会选 | 检查路径或注册表的信息来定义是否此次客户 |
| 俩止以下东什住分元成 | 端软件分发的任务完成           |

**注意**: 文件分发路径默认设在天珣中心和本地服务器安装目录下的 SDDownload 目录,所有的分发文件请在分发前都复制到此目录中。

#### 配置要点

- 1、 点击"添加"按钮设置策略;
- 添加一个任务分发 wireshack 抓包软件,并检查路径 c:\program files\abc 存在时完成软件分发任务;
- 3、添加 IP 组对客户端进行分发;
- 4、客户端在接收到策略后,弹出提示页面:

| 任务: test_20               | 1            |
|---------------------------|--------------|
| 是否执行软件分发任务                | ?            |
| 选择"执行",将立刻执彳<br>小时后将重新提示。 | 亍该任务。选择"等待", |
|                           |              |
| 空体(1)()                   | - 耕行(0)      |

5、点击"执行"后,进行软件正常安装:



| 7 Vireshark 1.2.0 (3 | 2-bit) Setup 📃 🗖 🗙   |
|----------------------|--|
|                      | Welcome to the Wireshark 1.2.0<br>(32-bit) Setup Wizard<br>This wizard will guide you through the installation of<br>Wireshark.<br>Before starting the installation, make sure Wireshark is not<br>running.<br>Click 'Next' to continue. |
|                      | Next > Cancel  |

### 13.2.3. 软件分发查询页面

| 软件分发  | 软件分发查询 | 软件分发默认参数  |
|-------|--------|-----------|
| 软件分发  | 查询     | tro.      |
| 任务名称  | 所有任务   | <u>辞期</u> |
| 分发状态  | 所有状态   |           |
| IP地址  |        |           |
| MAC地址 |        |           |
| 主机名   |        |           |
|       | 查询 重置  |           |

| 配置项:   | 说明  |  |
|--------|---|--|
| 任务名称   | 选择任务类型,分为" <b>所有任务"、"未过期任</b><br>务"和"已过期任务"以及每天策略的名称。 |  |
| 分发状态   | 选择软件分发任务的状态类型,分为" <b>所有状</b><br>态"、"等待分发"、"正在下载"等。    |  |
| Ip 地址  | 输入需要查询分发状态的终端的 IP 地址。                                 |  |
| Mac 地址 | 输入需要查询分发状态的终端的 MAC 地址。                                |  |



| 主机名 |
|-----|
|-----|

输入需要查询分发状态的终端的主机名。

可分别根据任务名称和分发状态,以及被分发的客户端的 IP 地址、

MAC 地址和主机名等条件进行查询。

点击"查询"进入详细查询页面:

| <b>医</b> 样分发瘤 | HILL   |          |      |              |            |           |            |
|---------------|--------|----------|------|--------------|------------|-----------|------------|
| 1040          | 0.0.00 | 11 11 10 | 1000 | 51101 IL 101 | 브라츠코       | 推動就產      | 0.040.000  |
| tastar        |        | 0        | 1    |              | 安装铝岩发      | 己解        | 2012-12-29 |
| fair and i    |        |          |      |              | 0.20 to 10 | 10.01278  |            |
|               |        |          |      |              | 7/12:0     | 10.000    |            |
|               |        |          |      |              | EMERNEDE   | 动电动脉      |            |
| # 1141        |        |          |      |              | 211-12     | 10.00     |            |
|               |        |          | 1.0  | 1. P. 1      | 并并且当先      | 11.0.1298 | 2012-31-04 |
|               |        |          |      |              | 如果到日来      | 0.0.0%    | 2012-10-04 |
|               |        | 10       | 1    |              | RED.H.     | 0.8:20    |            |

此页面显示的是该任务的分发状态及是否已完成。

再次点击"任务名称"进入详细任务状态查询页面:

| NU-UR    | C. BRIERING      | <b>NHHABUBH</b>   | 1001              |                     |              |          |                     |         |
|----------|------------------|-------------------|-------------------|---------------------|--------------|----------|---------------------|---------|
| 1no1_20  |                  |                   |                   |                     |              |          |                     |         |
| 11213    | STATES IN COLUMN |                   | RALEX .           | 出机部                 | 出现规范         | 主教法院     | 主要の小さけた日本生          | STREET. |
| 1441,2E  | PSHOT            | 18,301,500,1      | 11-20-22-32-32-33 | alkis-trail<br>1055 | <b>ESTE</b>  | 122.596  | THE WHERTTHE ROOM   |         |
| 1411_30  |                  | 18, 291, 309, 13  | 10-10-09-89-93-08 | 229828-356          | 正在部務所<br>門構成 | 101.375  | 714-8365/114-858    |         |
| 140,00   | ansis.           | 18.001.00.227     | EP-IC-DP-IL-TF-DF | Hatiooor<br>4       | 883XE        | 123, 265 | 114.000/114.00E     |         |
| 101,20   | STREET.          | 18, 991, 308, 325 | 19-10-29-09-47-83 | KIATURA MARKANA     | 1000         | 123.366  | 714.0065/116.00E    |         |
| 1605,00  | *#Res            | 18, 895, 166, 27  | 10-10-25-58-57-58 | 838-3 Marin<br>14   | tense.       | 10.36    | 714.000/216.000     |         |
| 00°22    | ****             | 102-28-294-6      | 10-20-22-82-10-31 | 20409-92            | 正方耳取用<br>戶籍以 | 133.369  | 114.3069,116.808    |         |
| 2007,200 | PRINT            | 18, 105, 19, 201  | 10-20-10-02-42-58 | man                 | 至在於和用<br>戶編以 | 10.08    | 714, 4363/714, 5185 |         |
| 1        |                  |                   |                   |                     |              |          |                     |         |

此页面可查询某台客户端进行此次软件分发的状态。

### 13.2.4. 软件分发默认参数页面





| 配置项:      | 说明                                    |
|-----------|---------------------------------------|
| 服务器带宽     | 输入用于软件分发的全局服务器最大带宽流<br>量,默认为 2000KB/S |
| 客户端带宽     | 输入用于软件分发的全局单台客户端最大带宽 流量,默认为 512KB/S   |
| 客户端上报时间间隔 | 设置客户端分发状态上报时间,默认为10分钟                 |

# 13.3. 短消息

### 13.3.1. 关于短消息

 短消息功能使管理员可以统一向客户端发送文字短消息,以行 使通知、提醒等功能。





| 配置项: 访 | 色明   |
|--------|--|
| 短消息标题  | 输入该条短消息的标题以便进行管理   |
| 短消息编辑框 | 短消息的内容,注意只能是文字内容   |
| 是否要求确认 | 要求用户是否需要对阅读的短消息进行确认;<br>选择"是",则客户端更新策略拿到短消息后,会弹<br>出消息阅读框,并且置顶显示,直到用户点击确认,<br>消息框才会消失;<br>选择"否",则客户端更新策略拿到短消息后,电脑<br>桌面右下角,会弹出消息提示,点击阅读;<br>无论选择"是"还是"否",短消息的阅读记录都会<br>从历史短消息中查询出来 |
| 授权发布单位 | 短消息发布的单位   |
| 正式发布时间 | 短消息发布的时间   |
| 重复发布周期 | 短消息重复发布的周期   |
| 生效截止日期 | 短消息生效的截止日期   |
| 策略应用对象 | 设置接收该短消息的 IP 组、工作组、主机名   |

### 13.3.2. 关于终端消息推送

终端短消息推送能使管理员精确的向一个或多个客户端实时推送文字短消息,以行使通知、提醒等功能。

#### 配置介绍

点击"客户端实时短消息"的"添加"按钮



| 客户端实时短消 | 有息   |   |
|---------|--|---|
| 短消息标题   | 中秋快乐!  |   |
| 短消息编辑框  | (最大字数限制100个汉字,禁止发布不正当言论!)                                |   |
|         | 月到中秋分外明,节曰喜气伴你行。人逢喜事<br>精神爽,人团家圆事业旺。节曰愉快身体硬,<br>心想事成您准赢。 | * |
|         |  |   |

| 配置项:   | 说明               |  |  |
|--------|------------------|--|--|
| 短消息标题  | 输入该条短消息的标题以便进行管理 |  |  |
| 短消息编辑框 | 短消息的内容,注意只能是文字内容 |  |  |
| 保存后如图  |                  |  |  |

| 1A型 <u>月读品包描述</u> |  |  |                |  |  |
|-------------------|--|--|----------------|--|--|
| 客户建实时短语息          |  |  |                |  |  |
| 69                |  | AB   |                |  |  |
| CARGIN.           |  | 20月間相比較,不再佳了眼,希希希<br>希希  | 30.031         |  |  |
| HOLANDER LAX      |  | 詳導者計與運用支生人物集成數 豆泥封<br>線大物約1%。由約2個約1%等項書<br>安生大物。由約2個熱力數 豆泥約%<br>者數 豆名是因飲自己 國家生產<br>用於定生人物第三方大物基件完主人物 | <b>R H H R</b> |  |  |
| 由载载重1.            |  | 月30中秋分外雨,节日春气尽参约。<br>人信息事者等何。人臣的回事近后。<br>节日偏使身体被,心想事话怎定再。  | 演送開            |  |  |

#### 选择需要发送的实时短消息点击"发送到"按钮

| 户情 | 印州址<br>印州址       | 使用人<br>- 结束口把给   |       | 御门 新典<br>主托告 | 日<br>日<br>日<br>日<br>日<br>日<br>日<br>日<br>日<br>日<br>日<br>日<br>日<br>日<br>日<br>日<br>日<br>日<br>日 |
|----|------------------|------------------|-------|--------------|---|
|    | 72.81至           | 15.6             | 東田人   | 20           | MACHENI   |
| 1  | ID 201-110-22    | sinia-774(31.65) |       |              | 00+00+29+52+52+30   |
| 1  | ID 201-254-10    | 458-8C           |       |              | 60-62-60-48-82-72   |
| 2  | ¥B 201.100 123   | VIII-TLTON RIGPL |       |              | 00-00-29-04-47-74   |
| 6  | 10.201.140.45    | daa-HC           |       |              | 00-24-81-58-33-3F   |
| 8  | 10.201.139.1     | ismenas-mj       |       |              | 00-10-25-90-84-5k   |
| 8  | 00.201.222.44    | #in=daa          | roph  | 4:-161.08    | 00-00-29-57-73-79   |
| 8  | 10.201.222.68    | ein-dae          | and . | #6:038->+    | 00-00-29-40-56-32   |
| 0  | 10.201.99.208    | ji 4099-7C       | axt   | #if36->a     | 00-28-18-68-40-50   |
| 0  | 172, 25, 89, 101 | Vervas           |       |              | 00-28-06-67-57-34   |
| 8  | 10.201.99.199    | ji un2003        |       |              | 0000239001088   |



勾选接收短消息的终端,然后点击发送就可以了。

## 13.4. 计算机名规范

### 13.4.1. 关于主机名规范

■ 主机名规范:为管理员提供了一种便利的手段管理整个网络中的主机名,使统一命名网络中的主机名成为可能。

| 主教的规范                    | 工作物名类和   |                             |         |     |          |
|--------------------------|--|-----------------------------|---------|-----|----------|
| 主机名规范                    |  |                             |         |     |          |
| 主机名称历名称                  |  |                             |         |     |          |
| 编述                       |  | *                           |         |     |          |
| 12.0                     |  | -                           |         |     |          |
| 20                       | <ul> <li>不应用主机名胡宝, 打算</li> <li>不应用主机名胡宝, 预止均</li> <li>应 直用主机名胡宝, 帮止均2</li> </ul> | 295±8.2<br>255±8.2<br>2±8.4 |         |     |          |
|                          | 11.81F   | 口油能                         | BAT HIM | 186 | 100      |
|                          | ASHSY SH   | 下载导入德斯                      |         |     | 浙洲一从最高市地 |
| 0845                     | 2.51   |                             |         |     |          |
| 0024                     | jing   |                             |         |     |          |
| 王· 前边 <del>和•</del> 月888 | 96.781.<br>  |                             |         |     |          |

| 配置项:    | 说明                           |
|---------|------------------------------|
| 主机名规范名称 | 输入该策略的名称                     |
| 描述      | 对该策略的描述                      |
|         | 选择"不启用主机名绑定,允许修改主机名",        |
|         | 则该客户端不启用主机名绑定,但可以任意修         |
|         | 改主机名。选择" <b>不启用主机名绑定,禁止修</b> |
|         | <b>改主机名"</b> 则该客户端不启用主机名绑定,但 |
| 选项      | 也不能修改主机名。选择" <b>启用主机名绑定,</b> |
|         | <b>禁止修改主机名"</b> 则该客户端启用了主机名绑 |
|         | 定,不能修改主机名。可以点击"从报表添加"        |
|         | 按钮获得相应的终端 ID、IP 地址、MAC 地址、   |
|         | 主机名。                         |

### 13.4.2. 配置要点

| 3.5.4100.417 | 主机采纳范   |                        |                  |                  |   |
|--------------|---|------------------------|------------------|------------------|---|
| Rit          |   |                        |                  |                  |   |
|              |   | -                      |                  |                  |   |
| 6.H          | C TERLENT- NA<br>C TERLENT- NA<br>* AMIL NET- MAD | 07354<br>67358<br>7355 |                  |                  |   |
|              | 1141 F  | 1.000                  | 91.53            | 245              | a li contra c |
|              | immar-um-waram-                                   | 00.000.148.1           | 1010/2012/1010 C | alitat (raspects | / ×   |
|              | ASSEA. SE   | 学被导入情報                 |                  |                  |   |
|              | 28  |                        |                  |                  |   |
| нала         |   |                        |                  |                  |   |

1、点击"添加"新建一个主机名规范,如下图所示:

2、点击"从报表添加"以添加绑定项。如下图所示:

| <u>从文件写入</u><br>「500」<br>下数写入機製<br>15日本知:<br>全部<br>E4本書和15年<br>在本語名的第日<br>在本語名的第日<br>日本語名的第日<br>日本語名の第日<br>日本語名の第日<br>日本語名の第日<br>日本語名の第日<br>日本語名の第日<br>日本語名の第日<br>日本語名の第日<br>日本語名の第日<br>日本語名の第日<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の第<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名の<br>日本語名<br>日本語名の<br>日本語名の<br>日本語名<br>日本語名<br>日本語名の<br>日本語名<br>日本語名<br>日本語名<br>日本語名<br>日本語名<br>日本語<br>日本語名<br>日本語名<br>日本語<br>日本語名<br>日本語名<br>日本語名<br>日本語<br>日本語<br>日本語名<br>日本語<br>日本語<br>日本語名<br>日本語<br>日本語<br>日本語<br>日本語<br>日本語<br>日本語<br>日本語<br>日本語 |                 |                   |                  |
|--|-----------------|-------------------|------------------|
| 11 HERETA  | 订熟址             | uar steld         | 184              |
| T1495980C-0051-4808-9066-0860087291861   | 10.201.20.17    | 00-0e-29-04-13-e4 | admin=774c31445  |
| 296575A9-9234-476C-8983-0073A3888968}  | 10.201.20.19    | 00-0e-29-31-12-4e | jingjus-154op    |
| (\$3040230-4246-4227-\$306-2575004FEACA)   | 10.201.20       | 5e-63-66-68-14-36 | sta-PC           |
| (190303110-0417-4173-4230-7484P9210307)  | 10.201.33.2     | 00-0e-29-a1-ab-89 | +uzzz-518c94044  |
| [] [74AFBEA1-1887-470C-8488-CD1847904858]  | 50.201.33.2     | 00-0e-29-2a-a3-8b | verue-518c94044  |
| CDC15188-0182-4278-5488-3288169C8180)  | 90. 201. 23. T  | 00-0e-29-23-12-s1 | win764-33-7      |
| [] [SORECTOT-9806-4768-6339-RESERLEDFIG]   | 10.201.33.22    | 00-Ge-29-18-De-34 | admin: yangesia  |
| C24944EB-1839-4096-1089-380604087F82   | 50. 201. 33. 27 | 00-0e-29-0è-1è-83 | VER-QUEBBORIERQ  |
| [] (20207377-4032-4395-9229-300738407002)  | 10.201.33.117   | 10-0c-29-3a-95-25 | VIR-MILITERNER   |
|  | 10.201.90.10    | 10-12-40-17-90-02 | THE DESIGNATION. |

5、选择想要绑定的终端项,点击"保存选择的项目"以保存,或点

击"保存所有的项目"。如下图所示:

| IRANE  | 1.*  |  |   |  |  |
|--|--|--|---|--|--|
|  |  |  |   |  |  |
| © TAMERANE- 1141<br>© TAMERANE- 941<br>* Orterane- 941 | 171158<br>171158<br>17158  |  |   |  |  |
| at age 1   | CP MIN   | BACININ  | 255   |  | 110  |
|  |  |  |   | 3.88   | ARAUN  |
| (1100FR21-1230-4409-4219-<br>4034471471861             | 10.001   | 0-0-0-0-0-0-0  | addie (angestie   | 1  | ×  |
| 21400002 - 2011 - 4823 - 6888-<br>685001219/81         | и ж. н п   | (R)=0.=(7)=(94-67)=+6.   | adare-176-31-00   | 1  | ×  |
| 23657549-9234-4755-6980-<br>8715468887081              | 18.000.001.99  | 0010-2016-72-06  | Jington PAm   |  | ×  |
| Indexes April 4227-1038-<br>Interpretation             | 18 205 39 20   | 5-651-0-1-0  | surfit.   | 1  | ×  |
| 300001034-0908-0178-0208-<br>1080499030071             | 18.201.10.2  | 00-0+-01-48-00   | 10000-52210000  | 1  | 8  |
| (11498140-1811-4100-4488-<br>0013-19066580             | 18 200 20 2  | 00-0-0+0+-0-05   | 10000-100-10000   | 1  | ×  |
| 100001188-0142-4219-0438-<br>3000.00020001             | 18.220.30.1  | 0010128-0210211  | 41474-31-7  | 1  | ×  |
| 20120727-0856-4709-0008-<br>8030031.0796()             | 18.005.10.22   | conterportente-te-   | alitie yngesie  | 1  | ×.   |
| 00004408-1870-0008-0088-<br>00004403/MNO               | 18 200 10 27   | 00-0-01-08-18-08   | 818-040808181185  | 1  | ×  |
|  | TRANS<br>TARASANS. 1944<br>TARASANS. 1944<br>TARASANS. 1944<br>TARASANS. 1944<br>TARASANS. 1944<br>TARASANS. 1944<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANS<br>TARASANSANS<br>TARASANS<br>TARASANS | 28.6.8.2         *           7.6.8.2.5         *           8.7.8.2.5 | TRANK         *           TRANK | TRANK         ************************************ | TRANK         ************************************ |

7、点击某客户端主机名修改主机并保存。



8、更新客户端规则以使策略生效。

### 13.4.3. 关于工作组名规范

工作组名规范:为管理员提供了一种便利的手段管理整个网络中的工作组名,使统一命名网络中的工作组名成为可能。

| 工作组名规范   |  |                          |                  |         |                 |
|----------|--|--------------------------|------------------|---------|-----------------|
| THREETER | 工作增高标志   |                          |                  |         |                 |
| R.I.     |  | Ť                        |                  |         |                 |
| BŘ       | CTAMINEARS. NAM<br>CTAMINEARS. NAM<br>FARINGERS. NAM     | 071784<br>071784<br>1784 |                  |         |                 |
|          | AT INCOME.   | 1788.0                   | - 1840, MI M     | TORA    | Control in such |
|          |  |                          | 0010-00-0-0-00-0 | 1015200 | / X             |
|          | 000000407500<br>00000407500<br>00000407500               | TREAME                   |                  | 6992041 | -               |
| NEAD     | 3CF0.400-047-042-028-1<br>00002940700<br>▲文月行入 二元世<br>主発 | FREARE                   |                  |         |                 |

| 配置项:    | 说明   |
|---------|--|
| 主机名规范名称 | 输入该策略的名称   |
| 描述      | 对该策略的描述  |
|         | 选择"不启用工作组名绑定,允许修改工作组   |
|         | <b>名</b> ",则该客户端不启用工作组名绑定,但可                                 |
|         | 以任意修改工作组名。选择" <b>个启用工作组名</b><br><b>绑定 禁止修改工作组名</b> "则该案户端不自用 |
| 选项      | 工作组名绑定,但也不能修改工作组名。选择   |
|         | "启用工作组名绑定,禁止修改工作组名"则   |
|         | 该客户端启用了工作组名绑定,不能修改工作   |
|         | 组名。可以点击"从报表添加"按钮获得相应   |
|         | 的终端 ID、IP 地址、MAC 地址、工作组名。                                    |

### 13.4.4. 配置要点

Ξŧ

| 工作组名规范         |   |                                   |                   |          |       |      |
|----------------|---|-----------------------------------|-------------------|----------|-------|------|
| INGUNTER       | Indano  |                                   |                   |          |       |      |
| SI.            |   | -                                 |                   |          |       |      |
| BR             | CTANICHARD IS<br>CTANICHARD IS<br>CANICHARD IS<br>CANICHARD IS  | -<br>8851084<br>9221084<br>931084 |                   |          |       |      |
|                | 14160   | 1744.0                            |                   | INRA     | 10000 |      |
|                |   |                                   |                   |          | 1.20  | 从科朱王 |
|                | 37CP41A50+0471+4402+4538+<br>0408238-4CTE30   | 10.001.140.27                     | 00/10/29-46/17-05 | ROMERCHO | 1     | ×    |
|                | #285A 38  | TREAGE                            |                   |          |       |      |
| HEAR           | 主用  |                                   |                   |          |       |      |
| NEA            | Jing  |                                   |                   |          |       |      |
| Station States |   |                                   |                   |          |       |      |
| 三十五之前+七四月四日    | Distance in the second s |                                   |                   |          |       |      |

1、点击"添加"新建一个主机名规范,如下图所示:

2、点击"从报表添加"以添加绑定项。如下图所示:

| 0408206407831  |                  |                   |            |
|--|------------------|-------------------|------------|
| 被除人型除了 的现在分词   |                  |                   |            |
| (1997년) (1997년) (1997년)<br>1987년 (1997년)<br>1987년 (1997년)<br>1987년 (1997년) | •<br>• [##] ##   |                   |            |
| 8088090 8086090  | 1726.00          | 和法国               | CARD CARD  |
| THANKARD - CONS - 4800- 1859 - 085000 TUSION                               | 10.001.00.17     | 00-029-64-10-s4   | NUMBER OF  |
| 12 12007104-F2H-ENE-0003-00730800900                                       | 48.003.00.19     | 00-0+-29-50-12-de | NUMBER     |
| E 100840030-4240-4207-5030-5075804493C4J                                   | 10 201 29 29     | 5-63-51-68-14-35  | vencencie  |
| E 198980109-048-4170-4200-TABOFER0011                                      | 18 201 00 3      | 00-0+-29-42-44-99 | NEGRO      |
| THATEMA-1887-4730-5848-1813438048582                                       | 10.001.33.1      | 00-01-28-24-42-59 | READER     |
| COLISION-DIAD 4810-DAM-SDARAGGERAD   | 10 201 30 T      | 00-0a-29-23-12-ai | VERSORADIO |
| E BODICES HOR WAR SOR RECEIPTIONS  | 10 201 39 22     | 00-0-028-18-84-34 | FERENCE!   |
| E Inserve and the second second second                                     | 10.201.53.27     | 00-0,-29-08-18-80 | VERICACIO  |
| Estation-rate rate acte-scattorenation                                     | 49, 201, 29, 117 | 00+0+-28+34-8k-2k | VENDORT    |
|  |                  |                   |            |

5、选择想要绑定的终端项,点击"保存选择的项目"以保存,或点

击"保存所有的项目"。如下图所示:

| 工作组名规表   |   |  |   |   |       |                            |
|----------|---|--|---|---|-------|----------------------------|
| INGRADAN | 工作副编辑员  |  |   |   |       |                            |
| nist.    |   |  |   |   |       |                            |
|          |   |  |   |   |       |                            |
| 34       | ○子用电工作组织和第一元5<br>○子用电工作组织和第一元5  | HURINES  |   |   |       |                            |
|          | POSTANDER, INC.   | CARD AT A BAS  |   |   |       |                            |
|          | * BRIDGER, MU   | 6041.40  | and a   | 1016  |       |                            |
|          | * BRISURFE RUS  | SPINE  | ( Married )   | 1.0116  | (ilin |                            |
|          | * BRIDGER, BUS  | 10.00.140.07   | 876-28-6- <b>7</b> -15  | E.O.1163<br>HALSAND                                 | -     | ) AMARA                    |
|          | * ARI DIANE - NU  | 00 EX 140 E<br>10 EX 140 E<br>10 EX 140 E                          | 80%-214-51-6<br>80%-214-51-6  | 2,011.61<br>90823009<br>90823007                    | -     | Amada<br>X                 |
|          | ANTING OF ALL AND     INVERSION AND     INVERSION     INVERSION     INVERSION     INVERSION     INVERSION     INVERSION   | 10. 201 140 A<br>10. 201 140 AT<br>10. 201 140 AT<br>10. 201 12 AT | Records and an<br>Record of the<br>Record of the Cold<br>Relation of the        | VOLDE<br>VOLDANY<br>VICEONY<br>VICEONY              |       | XNALX<br>X<br>X<br>X       |
|          | A BELL SUBJECT MUST      INTERNETING      INTERNETIN | 00. 201 (100 107 107 107 107 107 107 107 107 107                   | 80%20%4451%8<br>80%20%4451%8<br>80%20%16%52%4<br>80%20%16%72%4<br>80%20%16%72%4 | 3.01690<br>9063007<br>9053007<br>9053007<br>9053007 |       | x<br>x<br>x<br>x<br>x<br>x |

7、点击设置绑定的笔形编辑按钮修改某客户端的工作组名并点绿色

钩保存,再保存整个策略。



8、更新客户端规则以使策略生效。

注意:对于已经完成配置的策略可以选择"导出"到 excel 文件便于

修改。由该策略修改的主机名需要客户端重启后方能生效。

# 13.5. 远程文件删除

### 13.5.1. 关于远程文件删除

| 過程入計划隊                                 |   |  |  |                          |
|--|---|--|--|--------------------------|
| 前期名称                                   |   |  |  |                          |
| 演蹈描述                                   |   |  |  |                          |
|  |   |  |  |                          |
| 體除文件列表                                 | <b>文件</b> 編在  |  | 文件名称   | Sifi I                   |
| 医配方式<br>生物时间                           | 文件集任支持环境定量,用Svars形式表<br>情况匹配 -<br>● 新有时间 ○ I 作时间 ○ 事工作时间  | <del>. Кары</del><br>Октый   | (蜀十日東下的文件。<br>1  | 文件名称用•                   |
| 医酸方式<br>生物时间                           | 文件集任支持环境文量,用Sverskil d.表<br>情况区配 -<br>● 新有时间 ○ I 作时间 ○ 事工作时间<br>同门工厂  | т <b>Кары</b><br>  о цтна<br>  (1)[]   | 18-1877812(4)<br>1<br>1997 - 1997<br>1997 - 1997   | <u>定期</u><br>文件名新用•      |
| 医戴方式<br>生物时间<br>在领镜式                   | 文件器位支持环境交量,用#var#形式表<br>情况匹配。<br># 所有时间 《 工作时间 《 第工作时间<br>同志 工作时间<br>图 在规时生命 图 新规时生动  | н карани<br>о цтнай<br>Слуги   | 12 - 12 7 7 81 2 (*,<br>8<br>14 16 - 14 17<br>15 7 11  | <u>京開</u><br>文件名都用+      |
| 医氧力式<br>生物时间<br>在领情式<br>制能在用效象         | 文件製造支持研練文型、用Normanを引えま<br>構成正式 -<br>* 所有时间 ○ 工作时间 ○ 非工作时间<br>第二乙二二<br>「「在4月11」、「「素4月11」」<br>(注分有应用到任何対象) <u>工作</u> 22月13  | ★ 10月1日日<br>10以下时间<br>10以下时间<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月1日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月11日<br>10月111<br>10月111<br>10月111<br>10月1111<br>10月1111<br>11月1111<br>10月11111<br>10月1111<br>10月11111<br>10月11111<br>10月11111<br>10月11111<br>10月11111<br>10月11111<br>10月111111<br>10月11111<br>10月111111<br>10月111111<br>10月111111<br>10月111111<br>10月111111<br>10月111111<br>10月111111<br>10月111111<br>10月111111<br>10月1111111<br>10月11111111  | 1997 - 1997 - 1997 (*.<br>1997 - | <u>500</u><br>7(42,410)+ |
| 医副力式<br>全球时间<br>在球镜式<br>刻雕在用对象<br>印雕在型 | 文件基位支持环境实现,用Kreatel的过去。<br>精确匹配 -<br>* 新有时间 ① I作时间 ② 非工作时间<br>以下工厂<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一 | - 10月1日日<br>- 10日<br>- 10日<br>- 11日<br>- 11<br>- 1<br>日<br>- | ia - parreto, e.<br>1<br>1007 - entr   | 文件名称用。                   |

| 配置项:   | 说明                                   |
|--------|--------------------------------------|
| 策略名称   | 为该策略命名                               |
| 策略描述   | 该策略的详细说明                             |
| 删除文件列表 | 将要删除的文件信息添加到删除列表中,同时<br>可对多个文件进行删除。  |
| 匹配方式   | 精确匹配和模糊匹配。注: "精确匹配"要求<br>路径和文件名称准确无误 |
| 生效时间   | 可以选择"所有时间""工作时间""非工作时                |



|        | 间""以下时间段"生效,"开始时间"以及"约             |  |  |
|--------|------------------------------------|--|--|
|        | <b>束时间"</b> 仅对" <b>以下时间段"</b> 有效。  |  |  |
| 在线模式   | 选择该策略生效的网络场景,分为"在线时生<br>效"和"离线时生效" |  |  |
| 策略应用对象 | 关联到 IP 组、工作组、主机名使策略生效              |  |  |

#### 配置要点

1、点击"添加"远程文件删除策略,如下图:

| 运 把 文 <i>社</i> mi Ki                          |   |   |   |       |                |
|---|---|---|---|-------|----------------|
| 地在大竹開州  | ×.  |   |   |       |                |
| 解職名称  | teat  |   |   |       |                |
| 啊啊啊!!   | 1.0445  |   |   |       |                |
|   |   |   |   |       |                |
| 翻究注针列表  | 文件路径  |   | 业用 名祥   |       | 1.17           |
|   | C:\zhare  | abc   |   | . 2   | ML.            |
|   | E Vehare  | abe   |   | 1     | ×              |
| CBX53   | 文件路径支持环境安璧,用8va   | (4)到式表示,如果要制序数  | 个目录下的文件,                                      | 文件名称  | 1.87           |
| 但政方式<br>生物时间                                  | 文件描述文件环境交響,用x∞。<br>精確匹配 ・<br>● 新用时间 ○工作时间 ○ 1   | 「「「「「「」」」、「「」」、「」」、「」」、「」」、「」」、「」」、「」」、   | [个目录下的文件。                                     | 文件名称的 | 1+ <b>8</b> 7  |
| 匹配方式<br>生功时间                                  | 文祥路後支神环境英雄。用xxx<br>積積匹数 -<br>● 新聞封譯 ○ 工作时间 ○ 3<br>  | 本記式表示: 如果美術体製<br>本記(の) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1   | 不日季下的文件。<br>新報 田稔                             | 又件名称  | 1+ <b>3</b> ,7 |
| 匹戰方式<br>主帅时间<br>在场機式                          | 文件路後支持并構築度,用xxx<br>着稿匹数 -<br>※ 新聞封閉 〇 工作时間 〇 4<br>一方がけ戸<br>一方がけ戸<br>辺立相手生き 図 面積性な   | (4)式表示。如果要制作数<br>F工作时间(5)以下时间度<br>(5)(5)(5)   |   | 文件名称的 | (r.a.)         |
| 四戰方式<br>主帅时间<br>在场機式<br>前職应用対象                | 文件路後支件好構築欄,用www<br>精确函数 -<br>※ 所用时间 〇 工作时间 〇 4<br>日本17月7日<br>「2015年1月1日日日日日日日<br>「2015年1月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日  | (4)(武美示:如果要制)(4)<br>FI(10)(周)(3)(70)(周)(2<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521)(2)<br>(1521) | 个目录下的文件。<br>编辑 制格                             | 文件名称  | <b>6•表</b> 行   |
| 四級方式<br>主法时间<br>互張模式<br>修築应用21集<br>開始改算       | 文件路後支持好構築機,用xxx<br>着稿匹数 -<br>● 新育時間 〇工作時間 〇 4<br>日本時日<br>同時時日本 (2)高級社会<br>(社会有広用制任何対象) 宣告<br>全局   | (4) 式ま示:如果要制体数<br>につけば ○ 以下は自然<br>(たっけば)<br>(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)   | 个目录下的文件。<br>1943 mH8<br>1954                  | 文件名称  | <b>1</b> +3;7  |
| 四級方式<br>主法时间<br>互动技术<br>解释应用对单<br>回動式型<br>詞動者 | 文件路後支持并構築機,用xxx<br>着稿匹数 -<br>・ 新聞时間 〇 工作时間 〇 4<br>- 75591元<br>- 75591<br>- | (4)式表示:如果要制作数<br>EI 仰时间 ① 以下时间没<br>以上打开<br>一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一   | 小日本下的文件。<br>第4日 前日<br>5月 前日<br>5月<br>5月<br>5月 | 文件名称  | 1+ <b>3</b> 7  |

- 2、填写要删除的文件路径及文件名称,添加到删除文件列表
- 3、 点击"策略应用对象"->"查看及编辑"超链接,关联指定的 IP 组、 工作组、主机名
- 4、保存,更新策略。

# 13.6. 自动关机策略

### 13.6.1. 关于自动关机策略

自动关机策略能指定客户端的关机,同时可以指定客户端系统
 空闲时的等待关机时间,有效解决人离开了计算机没有关闭带
 来的管理弊端及风险。





| 配置项:     | 说明  |
|----------|---|
| 策略名称     | 为该策略命名  |
| 策略描述     | 该策略的详细说明  |
| 自动关机时间   | 指定终端计算机的关机时间(24 小时制,格式<br>hh:mm)                                    |
| 系统空闲关机时间 | 系统空闲时间指鼠标键盘没有输入操作的空闲<br>时间  |
| 生效时间     | 可以选择"所有时间""工作时间""非工作时<br>间""以下时间段"生效,"开始时间"以及"结<br>束时间"仅对"以下时间段"有效。 |
| 在线模式     | 选择该策略生效的网络场景,分为"在线时生<br>效"和"离线时生效"                                  |
| 策略应用对象   | 点击"查看及编辑"超链接,对象类型可以选择"IP 组"、"用户组"、"工作组"、"主机名"                       |



| 1 | 四种类型, | 选择相应的应用对象则启用自动关 |
|---|-------|-----------------|
|   | 机策略。  |                 |

配置要点

1、点击"添加"远程自动关机策略,如下图:

| 自动关机策略    | <u> </u>                                     |                        |            |
|-----------|--|------------------------|------------|
| 自动关机策     | 佫  |                        |            |
| 策略名称      | test   |                        | *          |
| 策略描述      | test if this<br>auto shutdown                | rule can control<br>n. | *          |
| 自动关机时间    | 23:30  |                        |            |
| 系统空闲关机时间  | 60   | 分钟(注:系统空闲指嗣            | 标,键盘都不操作的时 |
| 生效时间      | <ul> <li>回)</li> <li>⑥ 所有时间 ◎ 工作时</li> </ul> | 间 🖱 非工作时间 🖲 以下时        | 讨间段        |
|           | 开始时间   | 结束时间                   | 编辑 删除      |
|           | 2012-03-10 9:00                              | 2012-03-10 13:3        | 0 添加       |
| 在线模式      | 🗹 在线时生效 📝 离线                                 | 时生效                    |            |
| 策略应用对象    | (还没有应用到任何对象                                  | 2) 查看及编辑               |            |
| 创建类型      | 全局   |                        |            |
| 创建者       | jing   |                        |            |
| 注:右边有*号的U | 项目必须输入。<br>保存 取消                             |                        |            |

- 2、填写自动关机时间或系统空闲关机时间
- 3、点击"策略应用对象"->"查看及编辑"超链接,关联指定的 IP 组、 工作组、主机名。
- 4、保存,更新策略。

## 13.7. Win 防火墙例外

### 13.7.1. 关于 Win 防火墙例外

Win 防火墙例外可以设定指定应用程序进程,自动添加到
 Windows 防火墙的例外列表中。





| 配置项: 说 | .明   |
|--------|--|
| 策略名称   | 为该策略命名   |
| 策略描述   | 该策略的详细说明   |
| 例外进程列表 | 填写 Windows 防火墙例外的进程名   |
| 生效时间   | 可以选择"所有时间""工作时间""非工作时<br>间""以下时间段"生效,"开始时间"以及"结<br>束时间"仅对"以下时间段"有效。              |
| 在线模式   | 选择该策略生效的网络场景,分为"在线时生<br>效"和"离线时生效"   |
| 策略应用对象 | 点击"查看及编辑"超链接,对象类型可以选择"IP组"、"用户组"、"工作组"、"主机名"<br>四种类型,选择相应的应用对象则启用Win防<br>火墙例外策略。 |

#### 配置要点:

1、点击"添加"Win防火墙例外策略,如下图:



| 策略名称                   |  |  |            |
|------------------------|--|--|------------|
|                        | qq. exe  |  | *          |
| 策略描述                   | ବବ   |  |            |
| 例外进程列表                 | 进  | 程名称                                      | 编辑 删除      |
|                        | qq.exe   |  | 添加         |
| 生效时间                   | qq.exe<br>● 所有时间 ② 工作时间<br>开始时间<br>2012-03-10 9;00 | ◎非工作时间 ◎以下时间<br>结束时间<br>2012-03-10 13:30 | 段<br>编辑 删版 |
|                        | ☑在线时生效 ☑离线时  | 主效                                       |            |
| 在线模式                   |  | and the second                           |            |
| 在线模式<br>策略应用对象         | (还没有应用到任何对象)                                       | 查看及编辑                                    |            |
| 在线模式<br>策略应用对象<br>创建类型 | (还没有应用到任何对象)<br>全局                                 | <u>查看及编辑</u>                             |            |

2、点击"策略应用对象"->"**查看及编辑**"超链接,关联指定的 IP 组、 工作组、主机名,如下图。选择指定的 IP 组、工作组、主机名,并 "确定":

| Win防火   | 音例外                   |            |                    |               |
|---------|-----------------------|------------|--------------------|---------------|
| qq. exe |                       |            |                    |               |
| 对象类型    | IP组 ▼ 全部              | 青除         |                    |               |
| 对象选择    | 140                   | 1722545    | 99100              | 90            |
|         | 110                   | 222        | 20                 | 172.25.20.123 |
|         | 📝 172, 25, 1, 110-111 | 84         | 📝 172. 25. 22. 220 | 33            |
|         | 📝 254. x              | ☑mj主机      | 📝 172. 25. 85      | 99206         |
|         | <b>V</b> 42           | 10.201.251 |                    |               |
|         | 确定取消                  |            |                    |               |

- 3、"保存"并更新客户端规则。
- 4、 点击"开始"→"控制面板"→"Windows 防火墙"→"例外", 确认 QQ 已经被成功添加到 Windows 防火墙例外中,如下图:



| 😺 Vindows 防火墙 🛛 🔀   |
|---|
| 常规 例外 高級  |
| Windows 防火墙已关闭。您的计算机存在被外部源(如 Internet)攻击和<br>入侵的风险。建议您单击 "常规" 选项卡并选择 "启用" 。   |
| 程序和服务 (P):  |
| 名称  |
| <ul> <li>✓ AQT Remote Agent</li> <li>✓ DCOM</li> <li>✓ ESCC. Exe</li> <li>✓ Microsoft (R) Windows (R) Operating System</li> </ul> |
| <ul> <li>QQ2010</li> <li>QQ宠物启动程序</li> <li>QQ拼音手写输入工具</li> </ul>  |
| <ul> <li>✓ QQ拼音输入法词库安装工具</li> <li>✓ QQ拼音输入法积分等级程序</li> <li>✓ Q0拼音输入法皮肤安装工具</li> </ul>   |
| 添加程序 (26) [添加端口 (20) 編辑 (20) 删除 (20)  |
| 允许例外存在什么风险?   |
| 确定 取消   |

## 13.8. 终端实时操控

### 13.8.1. 关于终端实时操控

方便管理员主动连接至指定客户端查看和管理客户端服务、进程、网络连接、补丁信息等情况,以方便桌面运维。可以远程停止终端的服务、进程,可以更改远程终端相关服务器的启动方式,可以关闭远程终端的网络连接行为。也可以使用终端实时操作启用、禁用或删除指定终端的 IE 插件,管理员也可以用它来将指定的终端锁屏解锁,以及实时卸载客户端程序。

注意:"终端实时操控"的端口(UDP 7891)与应用准入端口相同。 如果安装天珣客户端但仍然无法验证通过,可以在"终端实时操控" 中输入该终端 IP 地址,如果无法查询则说明至客户端网络(UDP 7891)不通。



### 13.8.2. 服务页面

| <u>8</u> #4  | 1 网络这种        | 实时补丁查询  | 其插件管理 | 與湯發展 | 终端维护 |
|--------------|---------------|---------|-------|------|------|
| 尚容户端         | 服务信息          |         |       |      |      |
|              | itwich WAShip | ग्राहल  |       |      |      |
| T TRAFF IGHE |               | 10:144  |       |      |      |
| 致自动方式        | 自动            | - M2    |       |      |      |
| n            | 启动            | - R2    |       |      |      |
| m.e          |               | Later . |       |      |      |

| 配置项:      | 说明  |
|-----------|---|
| 客户端 IP 地址 | 输入需查询客户端的 ip 地址。                          |
| 更改启动方式    | 选中指定的服务,点击"更改启动方式"下拉<br>列表框,即可更改该服务的启动方式。 |
| 操作        | 选中指定的服务,点击"操作"下拉列表框,<br>即可更改该服务的状态。       |
| 服务名       | 输入"服务名"即可对指定的服务 <b>查询</b> ( <b>过滤</b> )。  |

说明:如果查询中提示"获取指定服务列表失败",有可能是网络超时所导致,请多次尝试。多次尝试失败说明至天珣客户端网络不通。

#### 配置要点

1、输入客户端 IP 地址,点击"查询",如下图:

| <b>8</b> 8      | 96                   | 网络连维                      | 308 | 补丁查询  | 11场件管理 | 新建築版制 | 经储藏物 |
|-----------------|----------------------|---------------------------|-----|-------|--------|-------|------|
| 查询客户            | 增服                   | <b>券信息</b>                |     |       |        |       |      |
| 注:*本功权<br>管户编环地 | dilliden<br>dilliden | 1点相称与習い事产<br>0、201.90,203 | 南元帅 | 10.00 |        |       |      |
| 要改 最助为;         | s 3                  | a ab                      | -   | - IRG |        |       |      |
| 操作              | 1                    | 8=D                       |     | WG .  |        |       |      |
| 服务会             |                      | 54L                       |     | 14:00 |        |       |      |

2、获得该客户端的服务列表如下:



| 10. ·             |      | FI              | ain supp                        | 188    | TIMP   | ow name Hater  | 85                                |
|-------------------|------|-----------------|---------------------------------|--------|--------|--|-----------------------------------|
| King:             | 户旗)  | <b>8.9</b> (1.9 | 6                               |        |        |  |                                   |
| 1.+876<br>5/%50*8 |      | 10.201.9        |                                 | 10     |        |  |                                   |
| EXALS             | 349  | 1843            | - 1                             | aver 1 |        |  |                                   |
| 80                |      |                 | - 1                             | WAC .  |        |  |                                   |
| 61.6              |      |                 | 6                               | 12     |        |  |                                   |
| -                 | 100  |                 | -                               |        | ammond |  | ALC: NO                           |
| 114               | ada  | UCN .           | Actival Japinika<br>Sectors (V) | 4.4    | #12r   | C. Window Capation 22 and don't win the a<br>adapticable comp  | LordDerroe                        |
| 15e               | 2444 | Sec.            | Adaptive Bright                 | 4.964  | Pitt   | $C_{\rm c}$ O find or a signature $20$ for close $t_{\rm can be statistically for the matrix on$   | ID ANTHORET<br>Tribergillerys     |
| 224               | id.i | anglive         | Application Rep-                | • #H   | 1F40   | C. Ukadara'nyyetan 22'anakana ana 16 a.<br>atawa   | Intelligence                      |
| 124               | 498  | 95×1            | Application Table               | 9.0    | 840    | C. Window Separate Winethors, and the later of the second se | W Anthonis<br>Viteralilaren<br>10 |
| -                 |      | ete.            | Apple catron lade               | 1017   | 平均     | C. Weakerstown (2016) and the state of a   | LondSpree                         |

3、选中需要更改启动方式的服务,并在下拉列表框中更改原服务启

动方式,即可成功更改服务的启动方式:

| 88         | i#W    | FIRE           | ALIN   393                        | BIH T   | 8.61 | I ILLANYS | TER IN HEARING                                      | IS SOUR OF                  | 1                                   |
|------------|--------|----------------|-----------------------------------|---------|------|-----------|---|-----------------------------|-------------------------------------|
| 查询容        | PMB    | R务信息           |                                   |         |      |           |   |                             |                                     |
| 1 · · 8 20 | end a  | 10. 201. 00.   | 007 <b>00 (1900</b> 1938)<br>2003 |         |      |           |   |                             |                                     |
| menanto    | nit.   | mek            |                                   | - 18    | 82   |           |   |                             |                                     |
| 80         |        | 10140          |                                   |         | 2    |           |   |                             |                                     |
| 804        |        | (後止)<br>第1日前13 |                                   | 10      |      |           |   |                             | ALL                                 |
| 0.62       | 1103   | esth)          | 10.15-15.00                       |         | 铁盐   | READLE    | 41  |                             | 10.01                               |
| 1214       | asliss | 629            | Artival Law<br>Malawill?)         | wills:  | 保止   | 18743     | C. Missing Copyright Con-<br>sized Weirage          | daret ma -k k               | landlystee                          |
| 1014       | Second | 214            | Adaptive Se                       | ightee. | 得止   | 949       | C 'Window'spetrall'se<br>and large tables a         | ducat see -b 1.<br>matters  | BT ANTROACT<br>This salitarys<br>24 |
| 22.8       | Anlice | dosp()+1       | Spplication<br>Lapon              | Exper   | 84   | 913       | E Windowshippstandifter<br>etamor                   | door, ees this              | locallystee                         |
| 104        | App31  | Qina.          | Application<br>15p                | Silvet  | 傳止   | 99.43     | C. Windows applied The<br>collection with Millegers | obact) war ob L<br>month wa | BT Ascherti<br>p'LocalDervi<br>se   |
| 184        | A2011  | av.            | Application.                      | Indur   | ierr | 9.65      | C Windows/apptaeds/ap                               | obout, eve "h a             | Localitettee                        |

 选中需要操作的服务名称,下拉列表框中选择服务的操作类型, 并点击确定,即可停止指定的服务。

### 13.8.3. 进程页面

### 配置介绍

|    | 870                  | 100       | 网络古根           | 实时补丁查翰   | 环境的资源                                   | - 44  | ANA    | H HANKERP | X     |
|----|----------------------|-----------|----------------|--|---|-------|--------|-----------|-------|
|    | 查询客                  | 户端进程      | 61.65          |  |   |       |        |           |       |
|    | 1: +3:0)<br>T(Piktri | teat 10.2 | 1              | en la mari   |   |       |        |           |       |
|    | 进程高                  |           |                | 20.00  |   |       |        |           | 17200 |
|    | 1112                 | 1000      | JI 17 2.10     | 10.01  |   | 11178 | JIL /4 |           | A14   |
|    | 4                    | 40816     | 36044          | C \Tears\Lasges\<br>50ze\bis\350ze e                       | Appillata'iKomong\i)<br>co              | 38    | lingan |           | 柳北    |
|    | z                    | .37100    | 30             | C.\Feers\Lisyaa\<br>50re\bis\350re.s                       | Ergenstehlen anglik<br>19               | 17    | lingue |           | 49.4L |
|    | 3                    | 5060      | Windwiify etc. | D: Weserskingensk<br>Hittikken hannen som V<br>Stiff: ense | AppData'doating\3<br>Er (Wahnail\38Daa# | 5     | ligner |           | 84.   |
|    |                      |           |                |  |   |       |        |           |       |
| ŀ  | 置项:                  | :         |                | 说明   |   |       |        |           |       |
|    |                      |           |                |  |   |       |        |           |       |
|    | N. MIL -             |           | t .            |  |   | )     |        |           |       |
| ÷) | 「''''」               | IP 地均     | Ŀ              | 输人需  | <b></b>                                 | 端日    | 勺ip地   | 址。        |       |
| _  |                      |           |                |  |   |       |        |           |       |
| 生利 | 呈名                   |           |                | 输入"  | 进程名"                                    | 即同    | 可对指    | 定的进       | 程查询   |

说明:如果查询中提示"获取指定进程列表失败",有可能是网络超



时所导致,请多次尝试。多次尝试失败说明至天珣客户端网络不通, 请检查客户端防火墙。

**重要:**强行杀除系统进程存在系统蓝屏、死机或数据丢失的现象,建 议慎重处理!

### 13.8.4. 网络连接页面

| 绩           | 激化                | 网络边接                 | SHHIT | EGA DEBARTU     | 198   HR | tiel¥ st      | atte  |      |             |
|-------------|-------------------|----------------------|-------|-----------------|----------|---------------|---|------|-------------|
| 查谢<br>副 • • | 客户编进<br>1980年1月11 | 接信息<br>MILLINEFEMALE | 47.77 | 41              |          |               |   |      |             |
| arrest a    | -ore to           | 1.211.90.201         | 2.4   | 1               |          |               |   |      | <b>死法</b>   |
| 1.120<br>1. | m                 | 10.201.00.202        | 12508 | 104.110.106.25  | 110      | 1182,3507     | C. Mragon Files, 1680/Wess<br>stady/Edgelot Severity/EE<br>CUEST, Eve | 81 H | (LANG       |
| τ.          | 717               | 10, 224, 30, 203     | 5297  | 10. 201. 1. 204 | (8533    | ETHELDE       | C Wragrap Filer Schlützte<br>met Eglinerinegilere ere                 | 都开   | URPH        |
| 8           | TOP               | 10.201.90.200        | 82409 | 10.201.1.204    | 9033     | REPORTS       | C.'dragues Files (588)/date<br>met Episce/seglare.es                  | 截开   | BRAR        |
| 4           | TOP               | 10.281.90.200        | \$248 | 10 201 1 204    | 8033     | ETHNESH       | C Mragram Files (200)Mate<br>rest Replacer's anglers and              | 新用   | <u>area</u> |
| 5           | TOP               | 18-201-80-205        | 52421 | 10.201 (1.204   | 8833     | ELISITS       | C. Grogram Files Suffiliate<br>mat Replaces's applers and             | 都政   | URAR.       |
| 置           | 项 <b>:</b>        |                      |       | 说明              |          |               |   |      |             |
| 户刘          | 端 IP              | 地址                   |       | 输入容到该约          | F户端的     | 的 IP 步<br>网络连 | 地址,点击 <b>"3</b><br>接情况。   | 查询   | ",即雨        |

**说明**:如果查询中提示"获取指定网络连接失败",有可能是网络超时所导致,请多次尝试。多次尝试失败说明至天珣客户端网络不通。

### 13.8.5. 实时补丁查询页面

#### 配置介绍

| 11.95<br>11.95              | 进程  | 网络连维                      | XNHT BE  | IE编件管理 | 经编数网                                       | 经编辑的         |  |
|-----------------------------|---|---------------------------|--|--------|--|--------------|--|
| 查询客                         | 户端实时  | 补丁信息                      |  |        |  |              |  |
| 1. entro                    | hill a state of the state of th  | A 19 GE 45-SHONES         | 108 F 19   |        |  |              |  |
| THE states was              | intrid in the second  | a talen // and / ar       | Contraction of the local division of the loc |        |  |              |  |
| <b>霍户横</b> 17               | 地址 10.2   | 01.90.263                 | 1000 A   |        |  | 22/83        |  |
| 幕/9 <b>8</b> 17<br>1733     | 10,2<br>Hates   | 01.90.203                 | 128  | 安支日期   | mit  | 88           |  |
| 幕/900127<br>1735<br>1       | 10, 2<br>11, 2<br>11, 2<br>11, 2<br>10, 2<br>10, 2<br>10, 2<br>10, 2  | 01.90.203<br>II           | 126<br>126   | 安美日間   | Security Update                            | 88           |  |
| ₩./*₩127<br>17.82<br>2<br>2 | 10, 2<br>13, 8<br>13, 8<br>13, 8<br>13, 8<br>13, 8<br>13, 8<br>13, 8<br>10, 9<br>10, 9 | 01.90.203<br>II<br>9<br>9 | <b>1</b> 125   | 安美日間   | Elif<br>Security Update<br>Security Update | <u>12.00</u> |  |

启明星辰 http://www.venustech.com.cn


| 配置项:      | 说明                                       |
|-----------|--|
| 客户端 IP 地址 | 输入客户端的 IP 地址,点击"查询"即可查询<br>到当前系统的补丁安装请况。 |

## 13.8.6. IE 插件管理页面

### 配置介绍

| 服务                  | 連程                    | 网络道         | <u>11</u>  | 家时补丁查翰    |               | 终端获解   | 推动维护                                      |                  |
|---------------------|-----------------------|-------------|------------|-----------|---------------|--|---|------------------|
| <b>に話</b><br>ま:***  | 件管理                   | NATA (887)  | 201百/14    | (F.))     | NR            |  |   |                  |
| 肩用                  | 成中的经件                 | 就用进中的管      | 217 (1911) | 活中的经济     |               |  |   |                  |
|                     | お行義                   |             | irs.       | 2.5       |               | 文件   |   | 1                |
| 15                  | CTSWeb5<br>ass        | SteMon Cl   | 周期         | Browser H | elper Object  | C:\Progra<br>201\TSW   | m Files (x86)/(Tencent'/Q/<br>ebMon64.dat | QPCMgr\4.7,1308. |
| 10                  | Google To<br>per      | oolbar Hel  | 崩          | Browser H | elper Object  | C:@rogram Files (x88)\Google/Google Toolbar\Googl<br>eToolbar 64.dl      |   |                  |
| 15                  | Google To<br>fier BHO | oolbar Noti | 剧          | Browser H | elper Object. | C: Program Files/Google/GoogleToolbarNotifier(5.7.6<br>db, 1642/sweb4.dl |   |                  |
| ]置                  | 项 <b>:</b>            |             |            | 说         | 明             |  |   |                  |
| 2 古 <del>如</del> 山山 |                       |             |            |           | 入客户端          | 的 IP 均   | b址,点击 <b>"</b>                            | <b>查询"</b> 即可    |
| -) :                | 410 <b>) 11</b> J     | 년 개.        |            | 到         | 当前系统          | 的 IE 指   | 盾件安装请况                                    | 10               |

### 配置要点

1、输入目标主机的 IP 地址,点击查询即可查看该终端的 IE 插件安

装情况。如下图所示:

| 服务            | 建粗 网络                      | 遊雅   | 实时补丁查翰    | LIMPER       | 终端获得                 | 推编维护                           | 6                             |
|---------------|----------------------------|------|-----------|--------------|----------------------|--------------------------------|-------------------------------|
| IE紙·          | 件管理                        |      |           |              |                      |                                |                               |
| 1: "<br>7 (14 |                            |      | (t,t)     |              |                      |                                |                               |
| a) a          | a de Martine III. 201.90.2 | 03   | 空街        | - AND        |                      |                                |                               |
| ALTER.        | BT6                        | ii.a | 2.5       | _            | 安祥                   | _                              |                               |
| 5             | CTSWebSiteMon Cl<br>ass    | 周期   | Browser H | elper Object | C:\Progr<br>201\TSV  | am Files (x86)<br>/ebMon64.dat | Tencent\QQPOMpr\4.7.1308.     |
| 8             | Google Toolbar Hel         | 周用   | Browser H | elper Object | C: Progr<br>eToolbar | am Files (x86))<br>_04.dll     | Google'sGoogle Toolbar\Googl  |
| 15            | Google Toolbar Not         | 剧    | Browser H | elper Object | C:VProgr<br>ab6.164  | am Files\Googl                 | e\GoogleToolbarNotiFier\5.7.6 |

选择需要处理的插件,点击"启用选中的控件""禁用选中的控件""禁用选中的控件"可对选择的插件做相应的操作。同时,"操作"项中将显示目前该插件的状态。如下图所示:



| 副新   | NE PES                  |             | 天时补丁查询 7    | II SAFE TO BE | 19 LA SOM              | Hidely  |
|------|-------------------------|-------------|-------------|---------------|------------------------|---|
| Ш    | 作管理                     |             |             |               |                        |   |
| TO N | UP#U 10.203.90.2        | 0.3         | 110         | NR            |                        |   |
| in.  | A00000 URA00            | 1998 I 1998 | 动动的 (1)     |               |                        |   |
|      | 558                     | 10.0        | .10         |               | 2.11                   |   |
| 1921 | CTSWebSiteHon Cl<br>ass | en.         | Browner Heb | ser Object    | C: 'Ptogra<br>2011/53W | en Files (x86)/Tennent/QQPCMgr\4.7.1306.<br>ebMon64.det |
| 23   | Google Toolbar Hel      | 5M          | Browner Hab | per Object    | C:'Progra              | m Files (x86)(Google)Google Toolbar(Google)             |

## 13.8.7. 终端锁屏

终端锁屏:对终端进行实时的屏幕锁定,管理员若发现某终端非 法接入或做出影响网络和其他终端安全行为时可对其进行及时 控制。

### 配置介绍

| 服务 进程 网络法维 实时补丁]<br>此对结网 | ân Hanten <mark>Haaff</mark> Kater                 |
|--------------------------|--|
|                          | Rida wali  |
| 配置项:                     | 说明   |
| 客户端IP地址                  | 输入客户端的 IP 地址,或"从终端发现里选择"需<br>要锁屏的终端,点击"锁屏"可以将终端锁屏。 |

### 配置要点

1、 输入目标主机的 IP 地址, 或者从终端发现里选择相应的主机, 如

下图所示:

| 终端银          | 1.用          |                               |  |                |
|--------------|--------------|-------------------------------|--|----------------|
| 注: "太        | UNEST A LENK | 计系统网络 网络索尔斯                   |  |                |
| 管户端目         | PHEN         | A ##                          | <b>以</b> 成領 10月  |                |
| _            | _            |                               | the second s |                |
| 101011       |              | RACIEN                        |  | <b>5</b> 8     |
| # She        | wClient Pag  | e — 网页拉话框                     |  | Rent.          |
| <b>#</b> 111 | m//10.201.1  | 204:8833/DesktopMgr/ShrwClier | tanpa -  |                |
| 从终来          | 省发现选择        | ŧ                             |  |                |
| IPHENE       | 1            | MACHEL                        | 主机集  | string.        |
| STREET       | 17           | HACIEN                        | 主机名  | and the second |

2、选择相应的客户端之后点击"锁屏"将该终端的屏幕锁定。同时,

被配置的条目将出现在本策略的配置页面上。管理员可以本页中



选择对终端解锁。

| 8.18 BAN                 |
|--------------------------|
| 8 M M                    |
| 21110                    |
|                          |
| und.asps%p+16.201.90.203 |
| 用的解决差码                   |
|                          |

## 13.8.8. 终端维护

## 配置介绍

| 服务    | 进程      | 网络连接              | 实时补丁查询                                       | IE插件管理                     | 终端颜屏  | 终端维护  |              |
|-------|---------|-------------------|--|----------------------------|-------|-------|--------------|
| 终端线   | 筆护      |                   |  |                            |       |       |              |
| 注: *本 | 功能对通过EX | <b>I 注接服务器的客户</b> | 端无效  |                            |       |       |              |
| 客户端工  | Pileti  |                   | 操作 卸载客户端<br>到载客户端<br>重启客户端<br>重启客户端<br>关闭终端电 | ▶ <u>執行</u> <u>基助</u><br>結 |       |       |              |
| 配置项   | į:      |                   | 说明   |                            |       |       |              |
| 客户端   | IP 地力   | Ł                 | 输入客户<br>序卸载。                                 | 端的 IP 地址                   | 止,或"卸 | 载"将该容 | <b>F</b> 户端程 |
| 操作    |         |                   | 卸载客户终端电脑                                     | 端,重启客                      | 户端,重  | 启终端电脑 | 前,关闭         |

# 13.9. 终端资源状况监控

## 13.9.1. 关于终端资源状况监控

 终端资源监控为管理员提供了一种资源使用率监控手段,可使 管理员及时了解终端的 CPU、内存、硬盘、网终的使用情况。
 配置介绍



| 终端资源状况监控    |                 |                     |
|-------------|-----------------|---------------------|
| 终端资源状态出     | i控              |                     |
| 策略名称        |                 | *                   |
| 策略描述        |                 | *                   |
|             |                 | *                   |
| CPU使用率      | ☑ 监控 高于 0       | ※时告警 (0为不告警)        |
| 内存使用率       | ☑ 监控 高于 0       | *时告警 (0为不告警)        |
| 硬盘剩余空间      | ☑监控 少于 0        | GB时告警(0为不告警)        |
| 网络数据包       | ☑ 监控 高于 0       | 时告警 (0为不告警)         |
| 网络字节数       | ☑ 监控 高于 0       | KB时告警 (0为不告警)       |
| 生效时间        | ◉ 所有时间 ◎ 工作时间 《 | ◯非工作时间 ◯以下时间段       |
|             | 开始时间            | 结束时间 编辑 删除          |
|             | 2012-03-10,9;00 | 2012-03-10 13:30 添加 |
| 在线模式        | ☑ 在线时生效 ☑ 离线时生  | 效                   |
| 策略应用对象      | (还没有应用到任何对象) 🔮  | 至看及编辑               |
| 创建类型        | 全局              |                     |
| 创建者         | jing            |                     |
| 注:右边有*号的项目如 | 2须输入。           |                     |
|             | 保存取消            |                     |

| 配置项:    | 说明  |  |
|---------|---|--|
| 策略名称    | 为该策略命名  |  |
| 策略描述    | 用于描述该策略的详细信息  |  |
| CPU 使用率 | 设置 CPU 使用率的告警值  |  |
| 内存使用率   | 设置内存使用率的告警值   |  |
| 硬盘剩余空间  | 设置硬盘剩余空间的告警值  |  |
| 网络数据包   | 设置网络数据包的告警值   |  |
| 网络字节数   | 设置网络字节数的告警值   |  |
| 生效时间    | 可以选择"所有时间""工作时间""非工作时<br>间""以下时间段"生效,"开始时间"以及"结<br>束时间"仅对"以下时间段"有效。 |  |
| 在线模式    | 生效时的网络场景,分为"在线时生效"和"离   |  |



|        | 线时生效"                   |
|--------|-------------------------|
|        | 点击"查看及编辑"超链接,对象类型可以选    |
| 等政应田对角 | 择"IP组"、"工作组"、"主机名"三种类型, |
| 東哈应用刈家 | 选择相应的应用对象则启用终端资源状况监控    |
|        | 策略。                     |

## 在 "信息中心" > "桌面运维" -> "终端资源使用状况告警" 查看告 警信息,如下图所示:

|             | and the second s | AN AD AD           |                  |         |           |
|-------------|--|--------------------|------------------|---------|-----------|
| a de Califi | 17.96.31   | LNEIN              | <u>\$645</u>     | 政策合意    | 1011-0.00 |
| BAT,        | 172 25 100 206   | 2010-7-26 23-21-11 | 网络教授包 51 44      | 円時数据包装管 | 科技業       |
| TAR.        | 172, 25, 100, 208  | 2010-7-28 28 21 30 | F08/F1740. 10.3M | 利益中平数分量 | 利於罪       |
| EAT,        | 172 25 100 235   | 2010/7-08 23 21:00 | 内存使用率 248        | 内存使用举音響 | 科技業       |
| TAR         | 172 25 100 205   | 0010-7-88 22 21:10 | 內存使用事 243        | 内存使用不管管 | NEE       |
| TAR .       | 172.25.100.006   | 2010-7-28-22-21-10 | 内は教養社、42-02      | 网络教教会由学 | 科技部       |
| TAR         | 112.25.100.206   | 2010-7-25 22:21:10 | FREFTER 6.34     | 网络宇节韵首要 | 利益要       |
| RAT,        | 172.25.100.205   | 2010-7-28 21 21:10 | 内存使用事 245        | 内存使用来自要 | 1475.00   |
| 7748        | 177.25.100.206   | 2010-7-28 21 21:10 | 网络教授者 动词         | 网络数据包括管 | 科技家       |
| TAR         | 172.25.100.208   | 0010-7-28 23 21:10 | 7967日数 6.98      | 网络学节数计管 | 利於臣       |
| TAS         | 172 25 100 208   | 2010-7-05 20-21-10 | 内存使用車 205        | 内存使用实质管 | #422.00   |

## 14. 认证管理

# 14.1. 第三方 CA 机构

第三方 CA 机构页面用于实现导入第三方 CA 机构根证书即其相关信息的功能,可用于在登录天珣用户控制的时候验证该 CA 机构颁发的用户证书。 点击"第三方 CA 机构"页面上的"添加"



| 第三方CA机构        |   |
|----------------|---|
| CA名称           | 第三方CA机构 *                                       |
| CA描述           | *   |
| 数字证书           | 上传证书  |
| 吊销证书列表         | 上传吊道证书列表  |
| 0CSP服务路径       |   |
| 证书状态验证         | ● 不验证证书状态 ○ 先进行在线验证,没有CA服务器或CA服务器不可用时使用吊销证书列表验证 |
| 是否启用           | ◎ 启用 ◎ 禁用                                       |
| 注: 右边有*号的项目必须输 | 保存 取消   |

| 配置项: 订    | 之明                        |
|-----------|---------------------------|
| CA 名称     | 填写易区别的名称                  |
| CA 描述     | 详细描述 CA 的相关属性             |
| 数字证书      | 点击右边的"上传证书"可以上传第三方根证<br>书 |
| 吊销证书列表    | 上传被吊销用户名的列表               |
| OCSP 服务路径 | 填写 0CSP 服务路径,用于在线验证证书状态   |
| 证书状态验证    | 可选择是否要验证证书状态              |
| 是否启用      | 配置启用还是禁用此根证书              |

# 14.2. 天珣 CA 机构

\*该章节功能仅适用于增强身份认证基础版和增强身份认证高级版

天珣系统自带轻量级的 CA,支持证书的生成、颁发,并且可以将证书颁发到 UKEY 介质中。



## 14.2.1. 天珣 CA 根证书

点击"天珣 CA 根证书管理"页面上"添加"按钮

| <u>天珣CA根证书</u> | 天珣CA用户证书   |   |
|----------------|------------|---|
| 天珣CA根证书        | <b>书管理</b> |   |
| 根证书名称          |            | * |
| 根证书描述          |            | * |
| 颁发者            |            | * |
| 注: 右边有*号的项     | 目必须输入。     |   |
| 生成并保存根证书       | 11 取消      |   |

"根证书名称"、"根证书描述"同"颁发者"都是必填项,可根据自身要求填写;点击"生成并保存根证书"时,弹出私钥保护密码输入框,校验一致后对证书的私钥部分进行加密。

| <u>天珣CA根证</u> | 長期CA用户证书 天珣CA用户证书 |
|---------------|-------------------|
| 天珣CA          | <b>艮证书管理</b>      |
| 请输入根证         | E书私钥保护密码:         |
| 密码:           |                   |
| 确认密码:         |                   |
| 注:密码可         | 1以为空              |
|               | 确定取消              |
|               |                   |

| 来自网页的    | 消息     | x   |
|----------|--------|-----|
| <u> </u> | 生成根证书成 | 功 ! |
|          | 3      | 确定  |



| 天珣CA根证书          | 天珣CA用户证书 |  |
|------------------|----------|--|
| 天珣 <b>CA</b> 根证· | 书管理      |  |
| 根证书名称            | test *   |  |
| 根证书描述            | test *   |  |
| 颁发者              | test *   |  |
| 注: 右边有*号的项       | 页目必须输入。  |  |
| 导出公钥证书           | 备份 刪除 取消 |  |

### 说明

- 天珣根证书页面仅可以创建一个根证书,根证书创建完成后,不可修改,但 可以删除或者备份;
- 天珣根证书私钥保护密码,管理员务必牢记,服务器不保存该密码;
- "备份"出来的根证书不能为第三方应用系统使用;若要使用此根证书,请
   使用"导出公钥证书"功能,可导出 cer 格式的根证书

## 14.2.2.天珣 CA 用户证书

| ENCARGEN   | 王重CA服户 | <b>维</b> 斯   |             |            |                                  |      |
|------------|--------|--------------|-------------|------------|----------------------------------|------|
| 天确CA用户证    | E#     | 148778 14    | Sana        | V 25.*/700 | 证书 团委东已常确的证书                     |      |
|            |        |              |             |            |                                  |      |
|            |        |              |             |            |                                  | 21.0 |
| RENDOR     |        | AN FEL MEDIA | REA         | 2558       | nam                              | H.K. |
| atmes<br>m | 444    | and to be a  | NAA<br>test | 2200A<br>B | (100)<br>2012-03-13 劉 2012-03-30 | HH   |

点击"天珣 CA 用户证书"页面上的"生成新证书"按钮



| 天珣CA根证书 | 天珣CA用户证书                                |                                    |                                |                    |                            |   |                          |                               |                                 |   |
|---------|---|------------------------------------|--------------------------------|--------------------|----------------------------|---|--------------------------|-------------------------------|---------------------------------|---|
| 生成新证书   |   |                                    |                                |                    |                            |   |                          |                               |                                 |   |
| 证书用户名   | test                                    |                                    | *                              |                    |                            |   |                          |                               |                                 |   |
| 部门      |   |                                    |                                | 选择                 | 部门                         |   |                          |                               |                                 |   |
| 邮件地址    |   | ?                                  |                                | 3                  | 三月,                        | 2012                                    |                          |                               | ×                               |   |
|         |   |                                    |                                |                    | $\simeq$                   | Β                                       |                          | >                             | *                               |   |
|         |   | *                                  | <                              |                    |                            | _                                       |                          |                               |                                 |   |
|         |   | 《周                                 |                                | _                  | =                          | Ξ                                       | 四                        | 五                             | 六                               |   |
| 有効期     | 0010 02 12                              | 《<br>周<br>8                        |                                | -                  | =                          | Ξ                                       | 四<br>1                   | 五<br>2                        | 六<br>3                          |   |
| 有效期     | 2012-03-13                              | 《<br>周<br>8<br>9                   | <<br>日<br>4                    | <br>5              | 6                          | 三<br>7                                  | 四<br>1<br>8              | 五<br>2<br>9                   | 六<br>3<br>10                    | * |
| 有效期     | 2012-03-13<br>注:右边有*号的项                 | 《<br>周<br>8<br>9<br>10             | <<br>日<br>4<br>11              | <br>5<br>12        | E<br>6<br>13               | Ξ<br>7<br>14                            | 四<br>1<br>8<br>15        | 五<br>2<br>9<br>16             | 六<br>3<br>10<br>17              | * |
| 有效期     | 2012-03-13<br>注:右边有*号的项<br><b>生成新证书</b> | 《<br>周<br>9<br>10<br>11            | <<br>4<br>11<br>18<br>25       | <br>5<br>12<br>19  | E<br>6<br>13<br>20         | 三<br>7<br>14<br>21                      | 四<br>1<br>8<br>15<br>22  | 五<br>2<br>9<br>16<br>23       | 六<br>3<br>10<br>17<br>24        | * |
| 有效期     | 2012-03-13<br>注:右边有*号的项<br><b>生成新证书</b> | 《<br>周<br>9<br>10<br>11<br>12      | <<br>4<br>11<br>18<br>25       |                    | 6<br>13<br>20<br>27        | <b>7</b><br>14<br>21<br>28              | 四<br>1<br>15<br>22<br>29 | 五<br>2<br>9<br>16<br>23<br>30 | 六<br>3<br>10<br>17<br>24<br>31  | * |
| 有效期     | 2012-03-13<br>注:右边有*号的项<br><b>生成新证书</b> | 《<br>周<br>9<br>10<br>11<br>12<br>时 | <<br>日<br>11<br>18<br>25<br>间: | <br>12<br>19<br>26 | 6<br>13<br>20<br>27<br>11: | <b>7</b><br>14<br>21<br>28<br><b>48</b> | 四<br>1<br>15<br>22<br>29 | 五<br>2<br>9<br>16<br>23<br>30 | デ、<br>3<br>10<br>17<br>24<br>31 | * |

点击"生成新证书"时,弹出根证书私钥保护密码输入框,校验一致后生成新的用户证书。

| 天珣CA根证书 天珣 | ICA用户证书  |
|------------|----------|
|            |          |
| 法统计组订并利用   | 21072523 |
| 请删入很证节档钥:  |          |
|            | 确定 关闭    |
|            |          |

**说明**:点击"生成新证书"时,如果是本地登录第一次点击,则会弹出根证 书私钥保护密码的输入框,如果不是本地登录第一次点击,则不要求输入根证 书私钥保护密码

插入 UKEY, 点击颁发到 UKEY, 弹出 pin 码校验框。



|   | 大词CA用户证书                                   |                   |                           |    |
|---|--|-------------------|---------------------------|----|
| test的证书   |  |                   |                           | 6  |
| 証料用户名   | [test                                      | 新行 ePass<br>現在需要強 | Token f<br>证您的用户 PIN 码。   | E  |
| 邮件地址  | testiftiert.com                            | RIPPIN:           | 「使用軟糖盘」                   |    |
| 状态<br>有效则                                       | 28<br>[2012-03-13] + [2012-03-             | 19502PDN          |                           | 聚消 |
| 证书颁发到【  | <b>########</b><br>JKey 成功,如下:             | <b>取</b> 約        |                           |    |
| 天珣CA根   | 证书 天珣CA用户i                                 | <u>E#</u>         |                           |    |
|   |  |                   |                           |    |
| test的   | 1证书  |                   |                           |    |
| <b>test的</b><br>证书用户<br>部门                      | 1证书<br>名 test                              |                   | 选择部门                      | 1  |
| <b>test的</b><br>证书用户<br>部门<br>邮件地址              | <b>注証书</b><br>名 test<br>ddd<br>test@test.c |                   | 选择部门                      |    |
| <b>test的</b><br>证书用户<br>部门<br>邮件地址<br>状态        | Y证书<br>名 test<br>ddd<br>test@test.c<br>正常  | <br>              | 选择部门                      | ]  |
| <b>test的</b><br>证书用户<br>部门<br>邮件地址<br>状态<br>有效期 | 1 証书 名 test ddd test@test.c 正常 2012-03-13  |                   | <b>选择部门</b><br>2012-03-30 | )  |

#### 说明:

- 第一次进入"天珣 CA 用户证书"页面时页面会提示安装 ActiveX 控件及启 明星辰安全证书。
- 天珣自带 CA 是轻量级的 CA,因此不单独提供和维护吊销列表。仅提供生成导出功能。
- Vista 以上系统运行该功能,须以管理员身份运行 IE。

天珣 CA 用户证书页面,点击"生成吊销列表"按钮,

|          |       | 新建任务 - http://10.201.1                | ,            |
|----------|-------|---------------------------------------|--------------|
| 请输入根证书私钥 | 保护密码  | 20120313134933.crl<br>未知大小 已完成マ       |              |
| 密码:      | ••••• | 😥 C:\Users\Administrator\Desktop\ 🛛 🏓 | 余:8.33GB 💌 🗎 |

## 14.2.3.天珣 CA 用户证书页面证书及 ActiveX 控件安装

第一次点击"天珣 CA 用户证书"页面时,页面会弹出需要安装 ActiveX 控件的提示,用于实现颁发证书到 UKey,现在详述 ActiveX 控件及证书的安装步骤,如下:

第一次去到"天珣 CA 用户证书"页面后,页面上弹出需要安装 ActiveX 控件的 提示

| 重天均内网安全风险管理  | \$P\$P\$計系统¥6.6.9.3 - ■i | cresoft Interne  | t Explorer |               |                     |             |
|--|--------------------------|--|------------|---------------|---------------------|-------------|
| 文件(12) 編編(12) 葺着   | 的 你那份 工具的 4              | 開算 (25)  |            |               |                     | 47          |
|  | 😚 🗩 指索 😒 收藏具             | e c  |            |               |                     |             |
| 地址 (0) 💼 http://10.200   | 1.211 00333/default.aspx | de de la companya de |            |               | . 🔁                 | 射到 結線       |
| <b>设</b> 为帮助保护您的安全,1   | sternet Explorer 已经停止)   | H此站点安美 Artiv   | # 拉件到您的计算机 | 拿击武处亚看法项      | -                   | ×           |
| 1000 F.H.  | 前朝安全风险管                  | 理与审计   | A.42       |               | 1                   |             |
|  | 11日新潟泉 20122             | 1883165000   | a to be a  |               | ing-系统操作员           | 000         |
| 「音页」   | THCARES                  | 天寶CA用户¥书   |            | 1 Still State | and a subsection of | 000         |
| <ul> <li>・ 0 安全系統</li> <li>・ 0 使人控制</li> <li>・ 0 安全規算</li> <li>・ 0 安全規算</li> <li>・ 0 守全規算</li> <li>・ 0 許の管理</li> <li>・ 0 許の管理</li> <li>・ 0 許法外親</li> <li>・ 0 部法外親</li> <li>・ 0 部法外親</li> </ul> | 天珣CA用户证                  | 书 生成   | 新亚松 生成为    | WERE .        | F 显示未吊脚             | e<br>Nets P |
| 图 0 杯碗审计   | 计预用户表                    | 2011   | MITTIEN.   | 像灰岩           | 是否活动                |             |
| 日の泉園法絶   | 100                      | velope   |            | istest        | 3                   | 201         |
| 日の以近ちな   | 1                        |  |            | tatest        | *                   | 3           |
| D天地CA机构  | 195                      |  |            | tatest        | 舌                   | 3           |
| □ 鼻侍认证   | durant                   |  |            | deliver.      | *                   | 1           |

右键点击弹出框并选择"安装 ActiveX 控件",注意名称

| Internet Explorer - 安全警           | 告 🛛                                   |
|-----------------------------------|---------------------------------------|
| 您想安装此软件吗?                         |                                       |
| 名称: UkeyCerMigrati                | on. cab                               |
| 发行者: <u>Beijing Venu</u>          | <u>stech Cybervision Co., Ltd</u>     |
| ≥ 更多选项 (0)                        | 安装 (I) 不安装 (Q)                        |
| -                                 |                                       |
| 来自 Internet 的文件可能<br>计算机。请仅安装来自您信 | 对您有所帮助,但此文件类型可能危害您的<br>任的发行者的软件。有何风险? |
| <b>v</b>                          |                                       |

点击"Beijing Venustech Cybercision Co..Ltd"进入"数字签名详细信息"页面,



## 再点击"查看证书"

| 01. 1. 211:8833/default. aspx    | 数字签名详细信息 ?  |
|----------------------------------|---|
| Internet Explorer - 安全警告         | <ul> <li>常规 高级</li> <li>数字签名信息<br/>该数字签名正常。</li> <li>签名人信息</li> <li>名称: Beijing Venustech Cybervision Co., Ltd</li> <li>电子邮件: 不可用</li> <li>签名时间: 2012年3月13日 18:59:12</li> </ul> |
| <u>cwh3</u><br>linguan4 test 101 | 查看证书 (V)<br>反签名   |
| liuyuan3 101                     | 签名人姓名:         电子邮件地址:         时间戳           VeriSign Tim         不可用         2012年3月13日 1  |
| <u>liuyuan</u><br><u>cwh2</u>    | 详细信息 @)   |
| <u>c*h1</u><br>22                |   |

跳到"证书"页面,点击"安装证书"

| 📆 证书信息       | 3.                                     |
|--------------|--|
| lindows 没有   | 足够信息,不能验证该证书。                          |
|              |  |
|              |  |
| 優发给:         | Beijing Venustech Cybervision Co., Ltd |
| <b>優发者</b> : | VeriSign Class 3 Code Signing 2010 CA  |
| 有效起始         | 日期 2011-1-24 到 2014-1-24               |
| 有效起始         | 日期 2011-1-24 到 2014-1-24               |







点击"是"后,会弹出证书安装成功的提示,这是说明证书已经安装成功了。

现在接着安装 ActiveX 控件,接着上述步骤,刷新该页面,然后再进入"天珣 CA 用户证书"页面,就会弹出一个安装插件的提示,

| Internet Explorer - 安全警告  |   |
|---|---|
| <b>您想安装此软件吗?</b><br>名称: UkeyCerMigration.<br>发行者: Beijing Venuste | cab<br>ech Cybervision Co., Ltd                   |
| ▼更多选项 (0)   | 安装 (L) 不安装 (D)                                    |
| 来自 Internet 的文件可能对统<br>计算机。请仅安装来自您信任的                             | 各有所帮助,但此文件类型可能危害您的<br>的发行者的软件。 <mark>有何风险?</mark> |

点击"安装",安装成功后,刷新该页面,就可以开始颁发天珣用户证书了。



# 14.3. 身份认证

\*该章节功能仅适用于增强身份认证基础版和增强身份认证高级版

## 14.3.1.关于身份认证

身份认证包括用户及证书信息管理和超级用户,用户及证书管理用于将用户及证书关联起来,此处的用户可以为天珣本地用户、AD 域用户及第三方 LDAP 用户; 超级用户页面用于规定网络认证的用户是否以名称为 TXAdmin 的超级管理员登录 windows 系统。

## 14.3.2.用户及证书管理配置介绍

以添加 AD 域用户为例。

(1) 先到"基本配置"的"用户组"里面配置相关的目录服务,详细配置请参考 4.10.2

(2)回到"用户及证书信息管理"配置页面,点击"第三方系统导入"

| 用户系统书籍总管理  | 超级用户       |            |              |       |      |
|------------|------------|------------|--------------|-------|------|
| 用户及证书      | 第三方系统导入 从5 | 2件导入 下载文件导 | 入復新          |       |      |
| 专业化        | mir-att    | 自己的        | ILS.         | 证书批约书 | 制定经端 |
| (Character | R          | 3878       | 4) Bai sones | sajia | 9    |
| 80.        | 22         | du         | da+          | duo.  |      |
| -          | 22         |            | sin          |       |      |
| <u>49</u>  | 27         | EAT 9      | 小马           | *3    |      |
| -          | 8          | #15        | **.          |       | 9    |

选择目录服务

| 電気<br>・の型工を注   | は利率形成。2012年0月31日発展<br>用产品は予約にある歴 4865月2 |   |            | , 当府曾想》: ===美術時作為 <u>600</u> |
|--|---|---|------------|------------------------------|
| <ul> <li>09111000</li> <li>402人日料</li> <li>0万分内計</li> <li>0717首様</li> <li>0月7首様</li> </ul> | *179550x25                              | Linkwithad<br>exc清式項目未開手 coo<br>HWTETETET | ENGD MA EN |                              |
| 0 0 0 12/10<br>0 0 12/2010   |   |   | 1755       | 目录新业的位                       |
| O HINKIT   |   |   |            |                              |
| OULEWR   |   |   |            |                              |
|  |   |   |            |                              |
| 04890  | 1                                       |   |            |                              |
| 0.50000  |   |   |            |                              |
| 02834  |   |   |            |                              |
| 0.60254  |   |   |            |                              |
| RHUESE   |   |   |            |                              |

选择对应的目录服务之后,点击"添加成员"按钮:



|  | LANDER, 2017/07/1010101  | · 二百万万万万 ● ● ● ●   |
|--|--|--|
| 875.W  | RPAUNIARS NORP   |  |
| 5 1 MH<br>\$1.254<br>\$1225<br>\$1710<br>\$1254<br>\$1254<br>\$1254<br>\$1254<br>\$1254<br>\$1254<br>\$1254<br>\$1254<br>\$1254<br>\$1254<br>\$1254<br>\$1254<br>\$1254<br>\$1254<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$1255<br>\$12555<br>\$12555<br>\$12555<br>\$12555<br>\$12555<br>\$12555<br>\$12555 | 日建湖克 新日<br>日建湖克 新日<br>王王王 Artistenhol<br>日王年58日 Artistenhol<br>日王年58日 Artistenhol<br>日王年58日  | Linue)<br>Activat  |
| () 第三方:() 第四   | - Common - C | D # R B R C  |
| 0天901488   | Buitte   | (BEPultin, BE-Lodernied, DE-tet  |
| O MINO E   | Contractor   | TB*Cognitiers, DD*2.sideration(, DD*er)  |
| 新有效学   | Stealin Centenillara   | 009Densis CentralDara 001Dislevithed 001set  |
| 5-500  | Foreigilamentgfastergala   | OM or signature to the second state of second s |
| PERSON   | Mar RP   | (Billings, RCLindershol, RCsat)  |
| in a second  | 128517   | ·····································  |
| 1+11   |  |  |

点击 "users", 选择用户, 勾选需要添加的用户, 然后点击 "**添加选择的项目**" 的按钮:

| 目录润                  | 数   差局                                  |   |
|----------------------|---|---|
| 日录服4<br>基本3¥<br>日录服4 | i linkeerk<br>detlinke<br>1856 CH=Toors | od<br>orknad, downost<br>DC-Dinderorkod, NC=nat           |
| 5                    |   | 的录影并其经  |
|                      | RE )                                    | 展開 (後多星元前100多记录,其他记录通来用过成条件进行者)() 華旗總算的項目                 |
|                      | 5.                                      | 目录路位  |
| 10                   | Aministrator                            | CS=Administrator, CS=Users, NC=Lindowerlead, DC=not       |
| 10                   | dae                                     | CSrdus, CH-Viers, DC-Linksorked, IC-tust                  |
|                      | Geant                                   | CS+Guert, CS+Upers, ID+Linkserkal, DC+net                 |
| 21                   | INSR_VERRS-EE7a00681                    | CN=DISE_VEROS-EETAOD681, CN=Uners, BC=Linkewsrkud, BC=net |
| 11                   | 11.01_718/15-127.400681                 | CH-IRAM_VERUS-HEVADD681, CH=Users, SC=Lindsverked, BC=ast |
| 25                   | line                                    | CS=jing, CS=Users, SC=Linkevrival, DC=net                 |
| 21                   | brittet.                                | CSvisitsgt, CHelliners, DC-Linkworkad, BCvnet             |
| -                    | esjin                                   | CS-majin, CS-Stern, SC-Linkeerkad, SC-net                 |

接着点击"目录浏览"旁边的"**返回**"按钮,跳转到此界面,再点击"**保存**"按钮,即可添加成功

| 用户及证    | E-166.0.17       | M E | CHRWA CHRWA | - Baugh (and and                         |  |
|---------|------------------|-----|-------------|--|--|
| 148 E A | 8% 原加成3<br>能使用的减 | 10  | *******     | · Malifier ( Ref. ) Ref.                 |  |
| TTR.    | 急期               | 8.6 | 0.584       | 8 <b>25</b> 488                          |  |
| 11      | £r               | duo | liniworked  | CBrdux, DH-Forrs, DCrijnikovskad, ICrost |  |

(3)将用户名称同证书名称进行绑定。点击对应的登录名:





| 20.20        | THE REPORT OF A DESCRIPTION OF A DESCRIP |                 |      |         |  |
|--------------|--|-----------------|------|---------|--|
| (Th)         | Shidone.   | 119168          | 1.5  | REMUTE: |  |
| 110)<br>110) | Br   | Linkworksd      | -    |         |  |
| be:          | \$   | Linkserland     | du   |         |  |
| 用户及证书信       | 息管理  | 超级用户            |      |         |  |
| 用户信息         | 编辑   |                 |      |         |  |
| 用户登录名        | lean -   |                 |      |         |  |
| 姓名           |  |                 |      |         |  |
| 用户类型         | Active D   | irectory Server |      |         |  |
| 目录服务         | dc=linkw   | orkad, dc=net   |      |         |  |
| 目录服务路径       | linkwork   | ad              |      |         |  |
| 部门           |  |                 | 选择部门 |         |  |
| 电子邮件         |  |                 |      |         |  |
| 证书用户名        | venus  |                 |      |         |  |
|              | 但在   | 制除取消            |      |         |  |

例如填写证书用户名 venus, 然后保存。 (4)如果需要为该证书绑定终端, 点击下图按钮

| 用户及证书 | 第三方系统导入 | 从文件导入 下    | 重文件导入模板 |       |          |
|-------|---------|------------|---------|-------|----------|
| 2.8.8 | 用户类型    | 0.9.6.6    | 単名      | 副用用いる | 101211-2 |
| nia.  | 27      | linkerlead | aia (   | PEN/D |          |
| day.  | D-      | liskerkst  | žae     |       |          |

点击"添加绑定终端"列的图标

| <b>美</b> 名 | avil        |          |     |             |            |
|------------|-------------|----------|-----|-------------|------------|
| 书用户者       | cataernand? |          |     |             |            |
| 產加弊定發展     | 臺酸造中增碳      |          |     |             |            |
| a - 4403   | AT HAM.     | 14238.92 | 主務名 | <b>把用</b> 人 | <b>2</b> 0 |
|            | 12          | む 東南     |     |             |            |

勾选想要绑定的终端 GUID, 点击"确定"按钮:



| 22 |   |              |                                |                   |      |    |
|----|---|--------------|--------------------------------|-------------------|------|----|
|    |   | 11111.96     | aciale.                        | 186               | #/用人 | 11 |
| 6  | (4P82CA23-5117-4303-8798-AB98582A0251)  | 10 201 20.33 | 00-0c-29-14-57-1s              | NDF-HACLPORCELI   |      |    |
| 6  | \$15331E8-6288-4188-4791-Fk188415582AT  | 10 201 20.25 | 00-0c-29-42-c8-HE              | NIN-TLIDHUNDERL   |      |    |
| 2  | (00000003E-215C-4CC4-8285-25104095C42D) | 10 201 20 51 | waraarbbribbreeree             | 78239-36437       |      |    |
| 5  | [BA4F5065-1000-4304-9302-BA084633674A]  | 10 201 20 13 | 00-0 <sub>6</sub> -29-64-13-#4 | ADMON-1114/201205 |      |    |
| 1  | [E00F100F-6010-45F1-0E02-AP0241EFE624]  | 10.201.20.11 | 00-26-18-62-40-63              | win2f9-lizezia.   |      |    |
|    | (PCH1825B-EATA-4092-3838-3484844514715) | 10 201 20 13 | 00-0-29-44-80-23               | ADMEN-114231305   |      |    |

然后在点击"保存"按钮,即成功绑定终端:

| 配置项: 说 | 明   |
|--------|---|
| 登录名    | 用于天珣用户认证取策略的帐号                                |
| 用户类型   | 用来表示该登录名是哪种用户类型,比如"本<br>地用户", "AD 域"或者"LDAP"。 |
| 目录服务   | 显示的是目录服务的名称。                                  |
| 姓名     | 仅是一个标记,其配置不影响功能的使用。                           |
| 证书用户名  | 证书用户名是颁发到 Ukey 里面的证书用户名称。                     |
| 添加绑定终端 | 某证书绑定了对应的终端之后,该证书只能在<br>绑定的终端上使用,其他终端不可使用该证书。 |
| 删除绑定终端 | 可以删除已经绑定的终端                                   |

#### 注意:

- ◆ 天珣本地用户不用另外导入,只需要在<u>基本配置→本地用户</u>页面添加完之
   后,就会自动出现在用户及证书页面;
- 天珣本地用户绑定证书可以按照上述方法绑定,也可以在基本配置→本地用
   户页面进行绑定。

## 14.3.3.超级用户

**超级用户**,即启用单点登录功能时,总是以管理员 TXAdmin 身份登录 Windows 系统的网络认证用户。用户可为天珣本地用户、AD 域用户和第三方 LDAP 用户。



### 添加超级用户的步骤如下:

在"超级用户"页面点击"选择用户",跳转到如下页面:

| 由 ●基本配置   | 用户及证书信息管理    超级用户  |
|---|--|
| <ul> <li>● ● 空本和直</li> <li>● ○ 安全基线</li> <li>● ○ 定全防护</li> <li>● ○ 花入控制</li> <li>● ○ 空全防护</li> <li>● ○ 补丁管理</li> <li>● ○ 許法外联</li> <li>● ○ 移动存储</li> <li>● ○ 終端审计</li> <li>● ○ 真面运维</li> <li>● ○ 认证管理</li> <li>● ○ 第三方 CA机构</li> <li>● ○ 景面 CA机构</li> <li>● ● 身份认证</li> </ul> | <b>选择用户</b><br>****请选择目录服务****<br>***请选择目录服务****<br>本地用户<br>linkworkad |

比如添加本地用户,选择对应的登录名之后,点击"确定"按钮:

| □●基本配置            | 用户及证书信。                               | 息管理 超级用户  |                  |       |
|-------------------|---------------------------------------|---|------------------|-------|
|                   | (s)                                   | 1.00  |                  |       |
| ■●准入控制            |                                       |   |                  |       |
| 10安全防护            | 日 示 浏 览                               | - 确定 ) 取消   |                  |       |
| の外工管理             |                                       |   |                  |       |
|                   |                                       |   | 本海               |       |
|                   | 登录名:                                  |   | 24               |       |
|                   | <u>登录名</u>                            | <u>姓名</u>   |                  |       |
| □□●移动存储           | admin                                 | s admin   |                  |       |
| 自●终端审计            |                                       |   |                  |       |
| □●桌面运维            | 8                                     |   |                  |       |
| □●认证管理            |                                       |   |                  |       |
| ●<br>第三方CA机构      |                                       |   |                  |       |
| ◎天珣℃△机构           |                                       |   |                  |       |
| 自然にす              |                                       |   |                  |       |
| <b>HOWE</b>       | 4                                     |   |                  |       |
|                   |                                       | A AN AT AS  |                  |       |
| 10基本配置            | 用户及证书信息管理                             | <u>840/87</u>   |                  |       |
| 10元工品紙<br>2.0注入形制 |                                       |   |                  |       |
| 0安全物护             | 启用单点登录功能时                             | ,以下用户总是以管理  | 员身份登录到客户端wi      | ndows |
| 2.0补丁管理           | 法异用户                                  |   |                  |       |
| 0资产管理             |                                       |   |                  | MEN   |
| 0年法外联             | 用户帐号                                  | 日子教師  | 1km              |       |
| - 中和和行籍           | adain.                                | 本地用户  | 10               | -     |
| の東面差距             | a a a a a a a a a a a a a a a a a a a | Contraction of the second s | 1. <del></del> . |       |
| 0 从证管理            | 3.                                    |   |                  |       |
| 回                 |                                       |   |                  |       |
| - O天珠CA机构         |                                       |   |                  |       |
|                   |                                       |   |                  |       |

| 配置项: 说 | 论明                  |
|--------|---------------------|
| 用户帐号   | 此处的用户帐号就是登录名。       |
| 目录服务   | 包括本地用户或者第三方系统目录服务。  |
| 操作     | 当点击"取消"时,则此条策略将被删除。 |

添加成功。

单点登录时,如果以该帐号或者该帐号关联的证书登录系统时,Windows 系统则 会以 TXAdmin 登录,并且该 TXAdmin 帐号具备管理员权限。



**注意:**如果你打包<u>单点登录客户端安装包</u>的时候,选择"Windows 本地登录帐号" 为"与网络认证相同的 AD 域帐号"时,就不会以 TXAdmin 帐号登录了,而只 会以该 AD 域帐号登录。

# 15. 信息中心

# 15.1. 关于信息中心

- 信息中心集中展现了终端的分布及受控状态、终端的资产报表、攻击告警及审计数据等重要信息,管理员可以在此处对终端的基本状况和策略配置后终端的执行状态进行详细查询,以便对策略运行的效果进行监督并根据报表进行改进。
- 在信息中心我们预置了超过 70 种不同的查询或统计报表,并
   通过各种条件的组合查询来满足不同用户的不同需求。在报表
   生成之后可以通过导出到 excel 方便对比和存档,每个报表在
   生成后都可将其设置为报表的首页,方便管理员实时查看。
- 接入信息:对终端设备运行状态统计,包括终端数量、在线数 量、受控数量、非受控数量和不合规数量等,以便于管理员实 时查看终端运行状况。
- 资产信息:显示上报的所有受控终端的资产信息,可详细查询 终端的硬件资产,也可查询安装的软件信息等。包括终端品 牌,CPU,主板,硬盘,内存,显卡,声卡,操作系统,指定软件,防 病毒软件等进行查询统计.
- **补丁信息**:对客户端补丁安装情况进行查询统计
- **审计信息**: 详细审计终端的各种行为,例如上网 URL、文件操 作、打印, 主机名, IP, MAC 变更, 等审计信息。
- 安全基线:详细审计终端所有安全基线违规的行为,例如强制
   补丁,进程管理,软件安装,防病毒软件,安全加固
- **外联控制:**详细审计终端设备非法外联,例如外设违规,多网卡



使用,异常路由

- **攻击告警**:记录一段时间内终端的 TCP/UDP 异常、流量异常、 ARP 欺骗发生情况等,并能详细记录终端的防火墙日志。通过 这些日志,管理员能轻松发现终端存在的问题并及时加以改 进。
- 移动存储:审计终端移动存储设备的操作行为
- 桌面运维:详细查询统计到终端资源使用状况和短消息阅读情况
- 级联报表:详细查询统计到所在单位的终端发现、补丁安装信息、补丁安装信息、安全基线违规终端、策略分发统计、资产信息操作系统以及主机类型统计的级联报表。

# 15.2. 接入信息

## 15.2.1. 配置介绍

对终端设备运行状态统计,包括终端数量、在线数量、受控数量、 非受控数量和不合规数量等,以便于管理员实时查看终端运行状 况。受控终端即已安装天珣客户端的终端。

#### 接入信息



| 配置项:  | 说明                                  |
|-------|-------------------------------------|
| 总终端数  | 所有子网中受控与非受控终端数合计                    |
| 在线数量  | 目前在线的终端数,同时包括受控与非受<br>控终端           |
| 受控数量  | 已安装天珣客户端的终端数量                       |
| 非受控数量 | 未安装天珣客户端的终端数量                       |
| 合规数量  | 受控终端中安全基线满足要求的终端数量                  |
| 不合规数量 | 受控终端中安全基线不满足要求的终端数<br>量             |
| 其他设备  | 网关,打印机,交换机,路由器,IP 电话等其他<br>类型的非受控终端 |

**注意**:一个子网中至少要有一台已安装天珣客户端的终端存在才能 发现这个子网中所有的其他终端的情况,

比如点击"受控数量"的数字链接,可以查看到所有受控的终端

| 1215-96.0             | NET.              | int ines:     |         |    | 25.6                | 1   | 8H 1 | 616163       | -      |                        |
|-----------------------|-------------------|---------------|---------|----|---------------------|-----|------|--------------|--------|------------------------|
| 10.1                  | SANTHER & TURA    | TRD: - AM     | -)/ THE |    | (<br>1.7.2)         | 100 | 5.00 | - WALLARD    | 100.00 | APP 127404450          |
| 11.00.00.00           | 30-0-02-09-02-01  | URLETTERING.  | +4047   | 10 | ******              |     | ×    |              |        | 1006/0010-10-16-27     |
| LITLI                 | 0.01210-0-01      |               | A1878   | -  | <b>Without Will</b> |     | 4    | Waters 20    | 141.00 | FURNING LODING         |
| a dai ta ar           | 10-0-0-0-19-01    | TRACTORNEE IN | -16/6   | 30 | deserver.           |     | 4    | dialog 7     | 4) 31  | AND DESCRIPTION OF A   |
| (Bi.n.H               | wird-wiels        | 10440277      | 488     | 10 | WARE DO             | 4   | *    | #10844 7 194 | 40.00  | 100/061117-019         |
| THE REAL PROPERTY AND | 12-12-12-12-12-12 | ID-AUTOMO     | 488     |    | Restance.           |     | 4    | Walnut Yorks | 42.31  | ACCREDING 1, SP. R. A. |
|                       |                   |               |         | -  |                     |     |      |              |        |                        |

再点击其中某台受控终端的 IP 地址链接,进入查看此台终端详细 信息的界面,即客户端报表



| 行状态 终端发现 并有    | <b>的设备</b> |              |             |                |     |  |  |
|----------------|------------|--------------|-------------|----------------|-----|--|--|
| 客户编结组 资产信息     | 进程         | 腦务           | 网络连撞        | 重新生成GUID       | 派回  |  |  |
| GUID           | (7)        | 495980C-C    | 051-4EC8-9D | 56-0E6DC872918 | (6) |  |  |
| 新聞創门           | 未知         | 1996日        |             |                |     |  |  |
| 使闯入            |            |              |             |                |     |  |  |
| 质凯印组           |            |              |             |                |     |  |  |
| 客户端网卡物理地址      | 00-        | 0c-29-84-f   | 3-64        |                |     |  |  |
| 客户端主机名称        | adr        | min-774c31   | dd5         |                |     |  |  |
| 上次的主机名称        |            |              |             |                |     |  |  |
| 再上次的主机名称       |            |              |             |                |     |  |  |
| IP地址类型         | 不易         | 椗            |             |                |     |  |  |
| IP地址           | 10.        | 10.201.20.17 |             |                |     |  |  |
| 上次的即地址         |            |              |             |                |     |  |  |
| 再上次的IP地址       |            |              |             |                |     |  |  |
| 策略系统用户登录信息     |            |              |             |                |     |  |  |
| 操作系统版本         |            |              |             |                |     |  |  |
| 操作系统语言版本       | 20         | 中文           |             |                |     |  |  |
| 上次下截第略时间       | 10/        | 26/2012 1    | 1:24:37 AM  |                |     |  |  |
| ServicePack主编号 | 0          |              |             |                |     |  |  |
| ServicePack副编号 | 0          |              |             |                |     |  |  |
| 安全状态           | 1          |              |             |                |     |  |  |

客户端报表显示了客户端的一些常见信息如部门信息、使用人、ip 地址等,对于同一个 MAC 地址,系统最多纪录最近3次的主机名和 IP 地址。还有客户端安全基线快照等信息。

页面中的"资产信息"请参照"资产管理",页面中的"进程","服 务","网络连接"请参照"桌面运维"-"终端实时操控"。

### 终端发现

通过组合条件查询终端信息



| 配置项:   | 说明  |
|--------|---|
| 部门     | 选择需要查询的部门信息,如果有设置部<br>门的话                         |
| 子网号    | 所有已发现的终端的子网号都将会显示出<br>来,选择其中一个进行查询                |
| IP 地址  | 输入要查询的终端 IP 地址                                    |
| MAC 地址 | 输入要查询的终端 MAC 地址                                   |
| 主机名    | 输入要查询的终端的主机名                                      |
| 是否受控   | 选择查询受控终端还是非受控终端                                   |
| 是否合规   | 选择查询合规终端还是不合规终端                                   |
| 是否活动   | 选择查询是否活动的终端                                       |
| 客户端版本  | 输入客户端版本号来查询特定版本的已受<br>控终端(只有选择了查询受控终端时此处<br>才能激活) |

## 选择特定条件,例如"所有受控终端"

| 终端表现            |                   |                   |           |     |                          |     |      |                        |
|-----------------|-------------------|-------------------|-----------|-----|--------------------------|-----|------|------------------------|
| Galagered       | MILLAN MILL       | RM    #/          | WIRSON    | 6   |                          |     |      |                        |
| eng, at set a   | in 179000 in in   | 4 = 350000 = 10 5 | TI ANIMAL | 131 | 95 <b>8</b> ) 27 (E4) 12 | 100 | 1600 | 100000000              |
| 10.201.01.17    | 10-1x-25-04 (D-14 | adelar MacDodd    |           | 33  | VIDEMAIDED               |     | ×    | 43.09.0002 11.04 77 44 |
|                 | 10-17-10-51-40-52 | /iwite-tt         |           | 39  | VIRGINALIZZED            |     | ~    |                        |
| 0.001 110.00    | Scitz-Mathematik  | numft             |           | 39  | 00004980                 |     | -    | 10/25/2012 4:03 10:09  |
| 1, 201, 222, 44 | 18-16-19-54-15-48 | eis-spieldi       |           | 39  | WARADADA                 |     | 1    |                        |
| TT.222.09.0     | 30-1x-22-a2-12-ia | REP-BATE/ORDED    |           | 38  | 100000                   |     | 1    | 10/10/0012 197 10:10 W |
| 1.001 A 107     | 30-02-02-04-01-TE |                   | *\$180    |     | 1                        | 4   | ×    |                        |
|                 | 10-02-02-07-02-08 |                   | ***       | 8   | 1                        |     | ×    | 14/36/04 2 25 - 10     |
|                 | 10-07-09-17-08-96 |                   | *#197     |     | 1                        |     | ×    |                        |
| E REL AN AN     | 81-12-12-14-17-16 |                   | 1985:211  | -   | 1                        |     | ×    |                        |
| 1.00.01         | 10-10-10-01-01-0  |                   | 921911    | -   | 1                        |     | ×    |                        |
|                 | 10-02-02-02-04-04 |                   | 10101     |     | 2                        |     | ×    | 11/91/0012 2:09 18 PM  |
| 6.011.3.201     | 10-12-02-98-02-44 |                   | *\$197    | 8   | 1                        |     | *    | 10/10/00111-01101      |
| 6.001.63        | 18-90-08-19-19-19 |                   | *\$180    | -   | 1                        |     | X    | 04/90/2021 1-00-57 19  |
| 1.11.11.2       | 10-18-48-87-48-00 |                   | *\$2080   | 8   | ,                        |     | ×    |                        |
| SHLEA           | 814240-0141-91    |                   | 12190     |     | 1                        |     | X    | 14/96/802 1-11-31-70   |
|                 | 101010-010-01     |                   | *121301   |     | 1                        |     | ×    | ALCOLOGIE 1 30 10 10   |
| AL 1881 17.993  | 10-12-42-02-12-44 |                   | 101121    |     |                          |     |      |                        |

点击其中的 IP 地址链接,同样可进入客户端报表查询界面



# 15.3. 资产信息

## 15.3.1. 配置介绍

查询统计终端资产信息的详细情况,包括终端的硬件资产和软件信息

| 资产信息         |                |
|--------------|----------------|
|              |                |
| 请选择查询统计图表类型: | ◎ 资产信息查询       |
|              | ◎ 按终端厂商品牌统计    |
|              | ◎ 按CPU型号统计     |
|              | ◎ 按内存大小统计      |
|              | ◎ 按内存大小查询      |
|              | ◎ 按硬盘大小统计      |
|              | ◎ 按硬盘大小查询      |
|              | ◎ 按硬盘型号统计      |
|              | ◎ 按网卡型号统计      |
|              | ◎ 按主板型号        |
|              | ◎ 按显卡型号统计      |
|              | ◎ 按声卡型号统计      |
|              | ◎ 按modem型号统计   |
|              | ◎ 按CD-ROM型号统计  |
|              | 💿 操作系统类型统计     |
|              | 💿 指定软件安装统计     |
|              | 💿 防病毒软件统计      |
|              | 💿 按主机类型统计      |
|              | 💿 终端操作系统安装时间查询 |
|              | 下一步 取消         |

#### 按主板型号

| 这产品量 |               |                          |
|------|---------------|--------------------------|
| 报表类型 | 積主概型号         |                          |
| 报表名称 | 技主板型局         |                          |
| 所奠部门 | 所有部门          | <ul> <li>选择部门</li> </ul> |
| 主板型号 |               | (同核制查询)                  |
| 图表类型 | ● 无图          |                          |
|      | C THATE       |                          |
|      | ② 構向柱状態       |                          |
| 创建状态 | 全局            |                          |
| 0024 | administrator |                          |
|      | 保存并执行 保存 执行   | 1952 取消                  |



| 配置项: | 说明                                 |
|------|------------------------------------|
| 报表类型 | 此报表的类型                             |
| 报表名称 | 此报表的名称                             |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 主板型号 | 输入要查询的终端的主板型号                      |
| 图表类型 | 选择图表类型,可选择"饼状图"和"横<br>向柱状图"        |

点击 **"执行"** 后

| 1824   |                                       | ×          |
|--|---------------------------------------|------------|
| 2743NCC  | 2                                     |            |
| 1518   | 1                                     |            |
| HIER Desittop Reference Platform   | 11                                    |            |
| 14738V?  | 1                                     |            |
| 155H-E73(HS-7636)  | 1                                     |            |
| 63M-E33 (MS-7680)  | 1                                     |            |
| 96C-M0/1333  | 1                                     |            |
| PSN73-AM   | 1                                     |            |
|  |                                       | 第1页/共有1页中的 |
|  | 1000 greater =                        | 2          |
|  | H 3118                                | 1          |
|  | A ADDIX Devictory Defor some Platform | 10         |
|  | <ul> <li>NORM-COMMS-20001</li> </ul>  | 1          |
|  | INCREMENT DIST. THEIR                 | 1 K        |
|  | PEGC-HW/LINE                          | 6          |
|  | # P9872-4H                            | 1.1        |
| and the second | 614                                   |            |

点击数字链接,可以查看到具体客户端

| 位主板型号<br>成次报表 [5:2001  |     |             |          |                            |                     |
|--|-----|-------------|----------|----------------------------|---------------------|
| and the second s | 教師為 | 18.33       | 01340    | RA XIII                    | PAIN                |
| 312 25 99 202  | łv  | LILIMUWN-PC | 66930000 | Nerosoft Windows 7 政<br>観察 | 2012-10-18 11:53:31 |
| 1  |     |             |          |                            | 第1四/共奏1页1条数据        |

注意:此处可导出图表到 excel

点击 IP 地址链接,可以查看该终端详细的资产信息。如:



资产ID: {A38D90C0-1E9F-4E2C-B8F7-B212CF9CEFC8}固定资产号: 导出到Excel

| ⊞ 资产信息 | 项目     | 值                                 |
|--------|--------|-----------------------------------|
|        | 名称     | 主机名测试1                            |
|        | 域      | WORKGROUP                         |
|        | 制造商    | ASUSTek Computer INC.             |
|        | 型号     | P5GZ-MX                           |
|        | 名称     | 主机名测试1                            |
|        | CPU数量  | 1                                 |
|        | 物理内存   | 2138222592                        |
|        | 用户名    | 主机名测试1\Administrator              |
|        | 项目     | 值                                 |
|        | 名称     | Microsoft Windows XP Professional |
|        | 版本     | 5.1.2600                          |
|        | 服务包版本  | Service Pack 3                    |
|        | 空闲物理内存 | 130180                            |
|        | 空闲页面空间 | 3421048                           |
|        | 空闲虚拟内存 | 2039452                           |

### 按终端厂商品牌统计

| 报表类型   | 接终端厂商品律统计                                |   |        |
|--------|--|---|--------|
| 报表名样   | 18981年—————————————————————————————————— | ) |        |
| Heri   | 所有部门                                     | • | 选择部门   |
| 「商品集名称 | 1  | a | の現制空向) |
| 图表类型   | ● 无图                                     |   |        |
|        | のは後期                                     |   |        |
|        | ◎ 編向推拔图                                  |   |        |
| 的建成态   | 全局                                       |   |        |
| 自動者    | administrator                            |   |        |

| 配置项:   | 说明  |
|--------|---|
| 报表类型   | 此报表的类型                                      |
| 报表名称   | 此报表的名称                                      |
| 所属部门   | 选择需要查询的终端所属的部门,也可点<br>击 <b>"选择部门"</b> 来进行选择 |
| 厂商品牌名称 | 输入要查询的厂商品牌名称,可模糊查询                          |
| 图表类型   | 选择图表类型,可选择 <b>"饼状图"</b> 和"横<br>向柱状图"        |



| R产版是                               |  |
|------------------------------------|--|
| <u>检修端厂商品牌统计</u><br>《改修计】写识别和 國內首法 |  |
| 1.9.68                             | 安装数  |
| Intel Corporation                  | 2  |
| 1                                  | 第10/共由101年8日<br>第10-11日<br>11日<br>11日<br>11日<br>11日<br>11日<br>11日<br>11日<br>11日<br>11日 |

## 按 CPU 型号统计

| 报表类型  | 接CPU型号统计  |  |                          |
|-------|---|--|--------------------------|
| 报表名称  | 核CPU型号统计  |  |                          |
| KWW1] | 所有部门  |  | <ul> <li>送保部门</li> </ul> |
| CPU型号 | The second se |  | (同樣構畫術)                  |
| 間未来到  | ◎ 无函  |  |                          |
|       | 四時間 (   |  |                          |
|       | 〇 橫向柱状图   |  |                          |
| 创建状态  | 全問  |  |                          |
| 包護者   | administrator   |  |                          |

| 配置项:   | 说明                                   |
|--------|--------------------------------------|
| 报表类型   | 此报表的类型                               |
| 报表名称   | 此报表的名称                               |
| 所属部门   | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择   |
| CPU 型号 | 输入要查询的 CPU 型号,可模糊查询                  |
| 图表类型   | 选择图表类型,可选择 <b>"饼状图"</b> 和"横<br>向柱状图" |

| 物合理》···································· |      |              |
|--|------|--------------|
| CPUSE                                    | 51   | 安装曲          |
| Intel Pentium III 关键器                    | 2534 | 1            |
| Intel Pentium III 先程書                    | 2600 | 1            |
| 1  |      | 第1页/出有1页2条数图 |

按内存大小统计



| 122.00        | 按应加非正式通知      |       |     |         |
|---------------|---------------|-------|-----|---------|
| INCOME.       | DU1197C/1900  |       |     |         |
| 推委名称          | 按内存大小统计       |       |     |         |
| 新興部门          | 新有限门          |       |     | 送祭御门    |
| 图表类型          | * 无图          |       |     |         |
|               | ◎ 第秋图         |       |     |         |
|               | ◎ 擁向柱状图       |       |     |         |
| 创建状态          | 全局            |       |     |         |
| 96 <b>8</b> 4 | administrator |       |     |         |
|               | 保存当地的         | et ta | 8.6 | <br>D B |

| 配置项: | 说明                                   |
|------|--------------------------------------|
| 报表类型 | 此报表的类型                               |
| 报表名称 | 此报表的名称                               |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择   |
| 图表类型 | 选择图表类型,可选择 <b>"饼状图"</b> 和"横<br>向柱状图" |

| 資产信息           |       |              |
|----------------|-------|--------------|
| 按内在大小统计        |       |              |
| 総合語社 四二四美 役为南法 |       |              |
| 68.5.6         | 11219 |              |
| 512H~1G        | 1     |              |
| 512网员下         | 1     |              |
| 1              |       | 第1页/共有1页2条修缮 |

#### 按内存大小查询

| 振表类型 | 按内存大小畫頭          |       |          |
|------|------------------|-------|----------|
| 报表名称 | UNITED U         |       |          |
| 所属部门 | 所有部门             |       | • 选择部门   |
| 内存大小 | ◎小子 ◎大子 ●介子      | MB至   | MB       |
| 创建状态 | 全局               |       |          |
| 创建者  | administrator    |       |          |
|      | <b>4</b> 2211110 | 16.67 | alte mat |



| 配置项: | 说明                                   |
|------|--------------------------------------|
| 报表类型 | 此报表的类型                               |
| 报表名称 | 此报表的名称                               |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择   |
| 内存大小 | 可直接输入小于或大于某个值的内存大<br>小,也可在一个内存大小区间查询 |

| 度内存大小贵海       |                 |                                       |        |                  |
|---------------|-----------------|---------------------------------------|--------|------------------|
| anger Sume    | Child (201      | 描述系统                                  | #0.188 | <b>冉在太小(MII)</b> |
| 172.25.42.111 | CLIENT2         | Microsoft Windows XP P<br>rofessional |        | 12B              |
| 192.108.1.4   | THINKPAD-1F7F8F | Microsoft Windows XP P<br>rofessional |        | 512              |
| 1             |                 |                                       |        | 第1页/共有1页2条数      |

**注意**:按内存大小统计和按内存大小查询的区别在于前者只按照实际上报内存的大小从数据库中读取出来并展现,而后者可以通过定义大小区间来展现,满足不同用户的需求。

| 按硬盘大小约 | 充计                |
|--------|-------------------|
| 资产信息   |                   |
| 报表类型   | 按键盘大小统计           |
| 报表名称   | 技硬盘大小统计           |
| 所属部门   | 新有部门 • 选择部门       |
| 图表类型   | ● 无图              |
|        | ◎阑趨               |
|        | ⑦ 摘向柱状图           |
| 创建状态   | 全局                |
| 创建者    | administrator     |
|        | 保存并执行 保存 执行 删除 取清 |
| 配置项:   | 说明                |
| 报表类型   | 此报表的类型            |



| 报表名称 | 此报表的名称                             |
|------|------------------------------------|
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 图表类型 | 选择图表类型,可选择"饼状图"和"横<br>向柱状图"        |



## 按硬盘大小查询

| 报表类型   | 接硬盘大小查询       |     |        |
|--------|---------------|-----|--------|
| 报表名称   | 按键盘大小查询       |     |        |
| 新聞銀门   | 所有部门          |     | • 送信部门 |
| 硬盘大小   | ◎小子 ◎大子 ◎介子   | GB室 | GB     |
| 的建状态   | 全局            |     |        |
| ette A | administrator |     |        |

| 配置项: | 说明                                   |
|------|--------------------------------------|
| 报表类型 | 此报表的类型                               |
| 报表名称 | 此报表的名称                               |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择   |
| 硬盘大小 | 可直接输入小于或大于某个值的硬盘大<br>小,也可在一个硬盘大小区间查询 |



| 拉硬盘大小查询       |                 |                                       |              |                  |
|---------------|-----------------|---------------------------------------|--------------|------------------|
| NARE PLAN     | 1020            | 操作系统                                  | <b>W</b> TER | <b>建</b> 盘水小(GB) |
| 172.25.42.111 | CLIENT2         | Microsoft Windows XP P<br>rofessional |              | 5                |
| 192.158.1.4   | THENKPAD-1F7F8F | Microsoft Windows XP P<br>rofessional |              | 5                |
| 1             |                 |                                       |              | 第1页/并有1页2册       |

## 资产信息查询



| 配置项:    | 说明                                 |
|---------|------------------------------------|
| 报表类型    | 此报表的类型                             |
| 报表名称    | 此报表的名称                             |
| 所属部门    | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 主机名     | 输入需要查询的主机名,可模糊查询                   |
| 主机类型    | 输入需要查询的主机类型,如"台式机"<br>和"笔记本"       |
| IP 地址范围 | 输入要查询的 IP 地址范围                     |





| 1  | tofessional<br>第1页/共有1页1条数据     |
|--|---------------------------------|
| (日本協会)<br>客产信息支援<br>「「市政法士」「日本副本」「日本副本」<br>「日本国本」「日本副本」<br>日本国本」<br>192,193,14 Didnk54<br>192,193,14 Didnk54 | D-1F770F Microsoft Windows X2 P |
| 使用人  | 输入使用人,客户端注册后才有此信息               |
| 指定软件名称   | 输入要查询的软件名称,多个软件通过"/"<br>来间隔     |
| 操作系统类型   | 选择操作系统类型                        |
| 资产报表更新时间   | 选择资产报表更新的时间                     |
| 硬盘大小   | 输入要查询的硬盘大小,可选择区间                |
| 内存大小   | 输入要查询的内存大小,可选择区间                |
| 网卡 MAC 地址  | 输入要查询的 MAC 地址,可模糊查询             |
| 网卡型号   | 输入要查询的网卡型号,可模糊查询                |
| CPU 型号   | 输入要查询的 CPU 型号,可模糊查询             |
| 固定资产号  | 输入要查询的固定资产号,可模糊查询               |
| 计算机序列号   | 输入要查询的计算机序列号,可模糊查询              |

**注意**:此处的查询属于一个综合报表自定义查询,通过各种不同的 组合条件,查询出符合用户需要的资产报表。

#### 按网卡型号统计

| 彩表击型 | 將同去戀是续讲       |         |
|------|---------------|---------|
| 振荡名称 | 被同中型号统计       |         |
| 新聞部门 | 所有却门          | • 选择部门  |
| 网卡型号 |               | (回模頻直得) |
| 西東東型 | ■ 元田          |         |
|      | ◎ 湖州田         |         |
|      | ② 偏向柱状图       |         |
| 的建状态 | 全局            |         |
| 自動者  | administrator |         |



| 配置项: | 说明                                 |
|------|------------------------------------|
| 报表类型 | 此报表的类型                             |
| 报表名称 | 此报表的名称                             |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 网卡型号 | 输入要查询的网卡型号                         |
| 图表类型 | 选择图表类型,可选择"饼状图"和"横<br>向柱状图"        |

| 按周末型号统计<br>编数数计 [53:2014] 最为前述       |              |
|--------------------------------------|--------------|
| <u>84184</u>                         | ISAU         |
| VMware Accelerated AND PCNet Adapter | 2            |
| 1                                    | 第1页/共有1页1条数组 |

## 按主机类型统计

| P. I.I. |               |        |
|---------|---------------|--------|
| 报表类型    | 按主机类型统计       |        |
| 报表名称    | 按主机类型统计       |        |
| 所属部门    | 所有部门          | ★ 选择部门 |
| 图表类型    | ◎秵            |        |
|         | 0 徽超          |        |
|         | ◎ 横向柱状图       |        |
| 创建状态    | 全局            |        |
| 创建者     | administrator |        |
|         | 保存并执行保存 执行    | 制除取消   |

| 配置项: | 说明                                 |
|------|------------------------------------|
| 报表类型 | 此报表的类型                             |
| 报表名称 | 此报表的名称                             |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |





|  | 图表类型                 | 选择图表类型,可选择"饼状图"和"横 |
|--|----------------------|--------------------|
|  |                      | 向柱状图"              |
|  | 原产简单                 |                    |
|  | 按主机类型统计              |                    |
|  | HACTOR COLOR (MANUES | 15.82              |
|  | N7cH                 | 2                  |
|  | 272 <b>5</b>         | 2                  |
|  | 1                    | 第1页/共振1页2条数谱       |

## 按显卡型号统计

| 资产信息           |               |    |    |    |         |
|----------------|---------------|----|----|----|---------|
| 报表类型           | 按盟卡型号统计       |    |    |    |         |
| 报表名称           | 按查卡型局统计       |    |    |    |         |
| 所属部门           | 所有部门          |    |    |    | • 选择部门  |
| 四卡亚号           |               |    |    |    | (同模構査谱) |
| 而未失型           | ● 光图          |    |    |    |         |
|                | © mare        |    |    |    |         |
|                | ◎ 構造柱状態       |    |    |    |         |
| 创建状态           | 全局            |    |    |    |         |
| 06 <b>2.</b> # | administrator |    |    |    |         |
|                | 保存并执行         | 保存 | 执行 | 删除 | 取消      |

| 配置项: | 说明                                   |
|------|--------------------------------------|
| 报表类型 | 此报表的类型                               |
| 报表名称 | 此报表的名称                               |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择   |
| 显卡型号 | 输入需要查询的显卡型号,可模糊查询                    |
| 图表类型 | 选择图表类型,可选择" <b>饼状图"</b> 和"横<br>向柱状图" |

| 位显于型号统计<br>编改统计 [异出图表] 國內商通 |   |       |                     |
|-----------------------------|---|-------|---------------------|
| 0.8.20                      |   | 2311Q |                     |
| VMware SVGA II              |   | 2     |                     |
| 1                           |   |       | 第1页/共有1页1条数图        |
| Ultrane SVGA II             | 2 |       | Allow constructions |



## 按声卡型号统计

| 資产信息 |               |    |    |      |         |
|------|---------------|----|----|------|---------|
| 松吉井型 | 披声卡型号统计       |    |    |      |         |
| 报表名称 | 被声卡型号统计       |    |    |      |         |
| 新業部门 | 所有部门          |    |    |      | 选择御门    |
| 声卡型号 | 4.<br>1000400 |    |    |      | (回號欄畫道) |
| 图表类型 | ◎ 天图          |    |    |      |         |
|      | 〇 饼状器         |    |    |      |         |
|      | ○ 横向柱状图       |    |    |      |         |
| 包藏状态 | 全局            |    |    |      |         |
| 北國者  | administrator |    |    |      |         |
|      | 保存并执行         | 保存 | 执行 | 1953 | 取消      |

| 配置项:   | 说明                                   |
|--|--------------------------------------|
| 报表类型   | 此报表的类型                               |
| 报表名称   | 此报表的名称                               |
| 所属部门   | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择   |
| 声卡型号   | 输入需要查询的声卡型号,可模糊查询                    |
| 图表类型   | 选择图表类型,可选择" <b>饼状图"</b> 和"横<br>向柱状图" |
| <u>校市 未理 号 統计</u><br>約計後计 [四出記書] (記2前後)<br>[1331]<br>Creative AudioPCI (E51371,E51373) (W<br>1 | 15日日<br>CM)                          |

按 modem 型号统计



第1页/共有1页0序盘提

I

| 报表类型             | 按modem型号统计    |         |
|------------------|---------------|---------|
| 报表名称             | 技modem型号统计    |         |
| 所属部门             | 所有部门          | → 选择部门  |
| Modem <u>型</u> 号 |               | (回模糊查询) |
| 图表类型             | ● 元图          |         |
|                  | 0 讲狱图         |         |
|                  | 0 備向柱状图       |         |
| 创建状态             | 全局            |         |
| 创建者              | administrator |         |

| 配置项:                                    | 说明                                 |
|---|------------------------------------|
| 报表类型                                    | 此报表的类型                             |
| 报表名称                                    | 此报表的名称                             |
| 所属部门                                    | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| Modem 型号                                | 输入需要查询的 modem 型号,可模糊查询             |
| 图表类型                                    | 选择图表类型,可选择"饼状图"和"横<br>向柱状图"        |
| 教主教教<br>技moden型行放计<br>和政策法 [G12版本] 强力服政 |                                    |

按 CD-ROM 型号统计

1


- 1

| 按CD-ROM型号统计   |   |
|---------------|---|
| 按CD-ROM型号统计   |   |
| 所有部门          | → 法择部门  |
|               | (可模糊查询)   |
| ●无图           |   |
| の変換           |   |
| ◎ 橫向柱状图       |   |
| 全局            |   |
| administrator |   |
|               | 按CD-ROM型号统计         按CD-ROM型号统计         新有部门         ● 无图         ● 无图         ● 新向柱状图         全局         administrator |

| 配置项:   | 说明                                 |
|--|------------------------------------|
| 报表类型   | 此报表的类型                             |
| 报表名称   | 此报表的名称                             |
| 所属部门   | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| CD-ROM 型号  | 输入需要查询的 CD-ROM 型号,可模糊查<br>询        |
| 图表类型   | 选择图表类型,可选择"饼状图"和"横<br>向柱状图"        |
| <u>株計算算</u><br><u>村CD-R0東型号検计</u><br>「総改設计」<br>S21回東<br>電力換表 | Bahy                               |

1

1

第1页/共有1页2毕数据

#### 操作系统类型统计

1

MATSHITA DVD-RAM U3862A

NECVMWar VMware IDE CDR10



| 根表类型 | 操作系统类型统计      |        |
|------|---------------|--------|
| 报表名称 | 操作系统共型统计      |        |
| 所屬創门 | 所有部门          | • 选择部门 |
| 西表类型 | ◎ 无器          |        |
|      | のは状態          |        |
|      | 《 構构性状图       |        |
| 创建状态 | 全局            |        |
| 创建者  | administrator |        |
|      | 保存并执行 保存 执行   | 創業 取済  |

| 配置项: | 说明                                 |
|------|------------------------------------|
| 报表类型 | 此报表的类型                             |
| 报表名称 | 此报表的名称                             |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 图表类型 | 选择图表类型,可选择"饼状图"和"横<br>向柱状图"        |
| 族产就意 |                                    |

| <u>操作系统类型统计</u><br>#29接注 [152][284] |              |
|-------------------------------------|--------------|
| <b>新在</b> 末端北部                      | 5687         |
| Microsoft Windows XP Professional   | 2            |
| 1                                   | 第1页/共有1页1条数据 |

#### 指定软件安装统计

| 报表类型   | 指定软件安装统计      |         |
|--------|---------------|---------|
| 报表名称   | 指定软件安装统计      |         |
| 所属部门   | 所有部门          | → 选择部门  |
| 指定软件名称 |               | (可模糊查询, |
| 图表类型   | ◎ 无图          |         |
|        | の詳述图          |         |
|        | ◎ 横向柱状图       |         |
| 创建状态   | 全局            |         |
| 创建者    | administrator |         |



| 配置项:   | 说明                                 |  |  |
|--------|------------------------------------|--|--|
| 报表类型   | 此报表的类型                             |  |  |
| 报表名称   | 此报表的名称                             |  |  |
| 所属部门   | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |  |  |
| 指定软件名称 | 输入要查询的软件名称,可模糊查询                   |  |  |
| 图表类型   | 选择图表类型,可选择"饼状图"和"横<br>向柱状图"        |  |  |

| 周定数件 安然统计<br>第四444 (2019年4月) 第五444 (2019年4月) |             |
|--|-------------|
| CD.S.R                                       | 11 M.M.W    |
| VMware Tools                                 | 2           |
| WINRAR 医魔化性 <b>制带器</b>                       | 1           |
| 大爆炸同使全的影響使用用什么改革产制                           | 1           |
| 法罪5  | 1           |
| #KQQ2009                                     | 1           |
| 380夜堂空士                                      | 1           |
| Aslobe Rasts Rayer 10 ActiveX                | ú           |
| PL-2303 USB-to-Serial                        | 1           |
| QQEITER 0 Petal                              | 1           |
| 1  | 第1页/共有1页9条数 |

#### 防病毒软件统计

| 报表类型     | 防病毒软件统计       |    |    |       |      |
|----------|---------------|----|----|-------|------|
| 报表名称     | 防病毒软件统计       |    |    |       |      |
| riman'i  | 所有部门          |    |    |       | 选择部门 |
| 允许延迟更新天教 |               |    |    |       |      |
| 國美美國     | ● 无图          |    |    |       |      |
|          | 〇 讲状图         |    |    |       |      |
|          | 〇 橫向柱状图       |    |    |       |      |
| 测建状态     | 全局            |    |    |       |      |
| 湖建省      | administrator |    |    |       |      |
|          | 保存并执行         | 保存 | 执行 | mittà | 服満   |

| 配置项: | 说明     |
|------|--------|
| 报表类型 | 此报表的类型 |
| 报表名称 | 此报表的名称 |



| 所属部门     | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择   |  |  |
|----------|--------------------------------------|--|--|
| 允许延迟更新天数 | 输入允许延迟更新的天数                          |  |  |
| 图表类型     | 选择图表类型,可选择 <b>"饼状图"</b> 和"横<br>向柱状图" |  |  |
| #####    |                                      |  |  |

| 防病毒软件统计<br>概念统计 [52:284] [经为新法] |     |     |              |
|---------------------------------|-----|-----|--------------|
| 机从用软件系列                         | 100 | 174 | 0.6          |
| Semannedtabil                   | 0   | 0   | 0            |
| nenos                           | 0   | 0   | 0            |
| IATIMA                          | 0   | 0   | 0            |
| Hollest State                   | 0   | 0   | 0            |
| R.F.BERA                        | 0   | 0   | 0            |
| THE TAON                        | 0   | 0   | 0            |
| 主要就需要審約目                        | 0   | 0   | 0            |
| 1                               |     |     | 第1页/共有1页7条数据 |

#### 按硬盘型号统计

| XI 1875 |               |         |
|---------|---------------|---------|
| 报表类型    | 按硬盘型号统计       |         |
| 报表名称    | 按硬盘型号统计       |         |
| 所属部门    | 所有部门          | → 送羅部门  |
| 硬盘型号    |               | (可模糊查询) |
| 图表类型    | ◎ 无图          |         |
|         | の単成的          |         |
|         | ○ 横向柱状图       |         |
| 创建状态    | 全局            |         |
| 创建者     | administrator |         |

| 配置项: | 说明                                 |
|------|------------------------------------|
| 报表类型 | 此报表的类型                             |
| 报表名称 | 此报表的名称                             |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 硬盘型号 | 输入要查询的硬盘型号,可模糊查询                   |





# 15.4. 补丁信息

# 15.4.1. 配置介绍

补丁信息可以查询统计终端补丁安装状态

| 青选择查询统计图表类型: |                    |
|--------------|--------------------|
|              | ◎ 指定终端补】安装状态查询     |
|              | ◎ 终端安装指定补丁状态查询     |
|              | ◎ 指定日期内客户端补丁安装状态查询 |
|              | ◎ 指定日期内未安装补丁的客户端查询 |
|              | ◎ 客户端补丁安装状态统计      |
|              | ◎ 补丁安装状态统计         |
|              | ◎ 安装失败补丁查询         |
|              | ◎ 部门补丁安装状态统计       |
|              | T IL BASK          |

#### 客户端补丁安装状态查询

| 报表类型 | 春户端补丁安装状态统计   |                          |
|------|---------------|--------------------------|
| 报表名称 | 赛户满种丁麦装状态统计   |                          |
| 所属部门 | 所有部门          | <ul> <li>选择部门</li> </ul> |
| 创建状态 | 全局            | 11                       |
| 创建者  | administrator |                          |
|      | 像存并执行 像存 执行 删 | 除取消                      |

配置项:

报表类型

#### 356

此报表的类型

说明

| 报表类型    | 终端安装指定补丁状态查询  |
|---------|---------------|
| 报表名称    | 终端安装指定补丁状态查询  |
| 所属部门    | 新有部门 • 法祭部门   |
| 靜輸入补丁号  |               |
| 青选择查询类型 | 要求安装已安装       |
| 刘建状态    | 全局            |
| 创建者     | administrator |

### 11 10.203.33 sin-#C 0.20 WORKOR AND 1 9 100% 100% 8 1 102 \$ 2 mm 第1页/共有2页15乐数据

点击数量链接,可以查看到具体补丁。

终端安装指定补丁状态查询

|                    | <u></u>             |               |                           |     |             |               |      |             |      |
|--------------------|---------------------|---------------|---------------------------|-----|-------------|---------------|------|-------------|------|
| GABA               | N-STATE R           | 2368          | and the local division of |     | ALC: NOTICE | 101 IL 102 IL |      | 0.0010-0105 |      |
| 19.20              | -598.               | 111111        | 1                         | TE  | STATISTICS. | 180           | 11.1 | EX          | 11   |
| 172.25.25<br>4.77  | ddd-PC              | WORKOR<br>CUP | 未知證<br>[]                 | 1   | 0           | R             | u.   | 100%        | 100% |
| 10.201.33.1<br>37  | WIN-NSJUTD<br>S9EM  | WORKOR<br>CUP | 前後用                       | 32  | 2           | 1             | 3    | 67%         | 33%  |
| 10.201.10<br>0.77  | jingjun-X54xp       |               | 的物质                       | 2   | 9           | 35            | 25   | 0%          | 100% |
| 10.201.22<br>2.88  | duo-PC              | WORKOR<br>CUP | mj                        | 82  | 8           | ₹.            | 1    | 100%        | 100% |
| 10.201.90.2<br>13  | Ikiyuan-PC          | 8             | -92                       | 83  | 0           | R)            | 8    | 100%        | 100% |
| 10.201.99.2<br>06  | jan99-PC            | WORKGR<br>OUP | <del>未知</del> 留<br>门      | 21  | 2           |               | 0    | 100%        | 100% |
| 172.25.25<br>4.101 | venus-638996<br>b45 | leason.co     | い東田                       | 22  | 0           | 8             | 8    | 100%        | 100% |
| 10.201.11<br>0.8   | XP64391738          | 3964          | nowitt                    | 135 | 2           | 1             | ш    | 100%        | 100% |
| 172.25.1.20        | t222                | WORKER        | 未知道                       | 1   | 0           |               | 2    | 100%        | 100% |

补丁草酮查普尔统)

| 报表类型 | 此报表的类型                             |
|------|------------------------------------|
| 报表名称 | 此报表的名称                             |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 图表类型 | 选择图表类型,可选择"饼状图"和"横<br>向柱状图"        |







| 报表名称    | 此报表的名称                             |
|---------|------------------------------------|
| 所属部门    | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 请输入补丁号  | 输入补丁的 KB 号                         |
| 请选择查询类型 | 选择"要求安装已安装""要求安装未安装"<br>等查询条件      |

#### 指定终端补丁安装状态查询

| 探表类型  | 操定经确补了安装状态置用  |                          |
|-------|---------------|--------------------------|
| 接责名称  | 指定终端补丁支装状态重调  |                          |
| PHONE | 0.0.0.0       |                          |
| 新國部门  | 所有部门          | <ul> <li>选择部门</li> </ul> |
| の理想を  | 全局            |                          |
| (注意)  | administrator |                          |

| 配置项:  | 说明                                 |
|-------|------------------------------------|
| 报表类型  | 此报表的类型                             |
| 报表名称  | 此报表的名称                             |
| 所属部门  | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| IP 地址 | 输入要查询的 IP 地址                       |

| BLAR .    | RADIES. | 2822     | GMARCH.  |
|-----------|---------|----------|----------|
| K82229593 | £       | <b>a</b> | 2        |
| KB873399  | 8       | <b>n</b> | <b>a</b> |
| KI0885635 |         | <b></b>  | 4        |
| x8885536  | +       | 臣        | 5        |
| 48680185  |         | #        | 2        |
| x20000113 |         | 青        | 8        |
| KB008302  | *       | 2        | 2        |
| KB890859  |         | 8        | 8        |
| ND091701  | . t.    | 22       | 2        |
| x80003756 | 4       | 吉        | 8        |

他工业和原则的通过



#### 补丁安装状态统计

| <u>朴」信息宣明与现计</u>   |   |  |  |  |
|--|---|--|--|--|
| 报表类型   | 补丁安装状态统计  |  |  |  |
| 报表名称   | 补丁安装状态统计  |  |  |  |
| 新宣教门   | 17+-m17   |  |  |  |
|  |   |  |  |  |
| H1H2A208   | ●最近7 <u>天</u>   |  |  |  |
| <b>肉</b> ±★用   | E RE MO   |  |  |  |
| MAX <del>X</del>   | ◎ 无图  |  |  |  |
|  | の讲述图  |  |  |  |
|  |   |  |  |  |
|  | 10 横向柱状图  |  |  |  |
| 创建状态   | 全局  |  |  |  |
| 创建者  | administrator   |  |  |  |
|  |   |  |  |  |
|  | 保存并执行 保存 执行 删除 取消   |  |  |  |
|  |   |  |  |  |
| 配置项:   | 说明  |  |  |  |
| <b>报表类型</b>  | 此报表的类型  |  |  |  |
|  |   |  |  |  |
| 报表名称   | 此报表的名称  |  |  |  |
|  | 选择雲要查询的终端所属的部门。   |  |  |  |
| 所属部门   |   |  |  |  |
| ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,  |   |  |  |  |
|  | 击 <b>"选择部门"</b> 来进行选择   |  |  |  |
| 时间范围   | 击 <b>"选择部门"</b> 来进行选择<br>   |  |  |  |
| 时间范围   | 击"选择部门"来进行选择<br>选择统计的补丁安装时间范围   |  |  |  |
| 村间范围   | 击"选择部门"来进行选择<br>选择统计的补丁安装时间范围<br>选择图表类型,可选择"饼状图"和"横   |  |  |  |
| 时间范围<br>图表类型   | 击"选择部门"来进行选择<br>选择统计的补丁安装时间范围<br>选择图表类型,可选择"饼状图"和"横<br>向柱状图"  |  |  |  |
| 时间范围<br>图表类型   | 击"选择部门"来进行选择<br>选择统计的补丁安装时间范围<br>选择图表类型,可选择"饼状图"和"横<br>向柱状图"  |  |  |  |
| 时间范围<br>图表类型   | 击"选择部门"来进行选择<br>选择统计的补丁安装时间范围<br>选择图表类型,可选择"饼状图"和"横<br>向柱状图"  |  |  |  |
| 时间范围<br>图表类型<br>四篇章章章鉴述  | 击"选择部门"来进行选择<br>选择统计的补丁安装时间范围<br>选择图表类型,可选择"饼状图"和"横<br>向柱状图"  |  |  |  |
| 时间范围<br>图表类型   | 击"选择部门"来进行选择<br>选择统计的补丁安装时间范围<br>选择图表类型,可选择"饼状图"和"横<br>向柱状图"  |  |  |  |
| 寸间范围 图表类型 TERMS #5%社 TERMS #5%H T  | 击"选择部门"来进行选择<br>选择统计的补丁安装时间范围<br>选择图表类型,可选择"饼状图"和"横<br>向柱状图"  |  |  |  |
| 时间范围<br>图表类型<br>TINKE #5%社<br>#TEXE #5%社<br>#TEXE #5%社<br>#TEXE #5%社   | 击 <b>"选择部门"</b> 来进行选择<br>选择统计的补丁安装时间范围<br>选择图表类型,可选择" <b>饼状图"</b> 和"横<br>向柱状图"  |  |  |  |
| 寸 间 范 围<br>図 表 类 型<br>「 取 数 2 B 5 W 社<br>本 1 安 業 共 高校社<br>本 1 安 業 共 高校社<br>本 2 2 2 2 5 5 3<br>K8 2 2 2 5 5 3<br>K8 2 2 3 5 5 3<br>K8 2 4 2 4 5<br>K8 2 4 2 5 2 5<br>K8 2 4 2 4 5<br>K8 2 4 2 5 2 5<br>K8 2 4 2 4 5<br>K8 2 4 2 5 2 5<br>K8 2 4 2 5 2 5<br>K8 2 4 2 5 2 5<br>K8 2 4 5<br>K8 2 4<br>K8 4<br>K8 4<br>K8 4<br>K8 4<br>K8 4<br>K8 4<br>K8 4<br>K8 4<br>K8 4   | 击"选择部门"来进行选择<br>选择统计的补丁安装时间范围<br>选择图表类型,可选择"饼状图"和"横<br>向柱状图"  |  |  |  |
| 中间范围       図表类型       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII   | 击"选择部门"来进行选择       选择统计的补丁安装时间范围       选择图表类型,可选择"饼状图"和"横       向柱状图"   |  |  |  |
| 时间范围<br>图表类型<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESENSION<br>TERESEN | 击 <b>"选择部门"</b> 来进行选择<br>选择统计的补丁安装时间范围<br>选择图表类型,可选择" <b>饼状图"</b> 和"横<br>向柱状图"  |  |  |  |
| 时间范围       S表类型       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII   | 击"选择部门"来进行选择       选择统计的补丁安装时间范围       选择图表类型,可选择"饼状图"和"横       向柱状图"   |  |  |  |
| 时间范围       STEREE        STEREE  | 击"选择部门"来进行选择         选择统计的补丁安装时间范围         选择图表类型,可选择"饼状图"和"横         向柱状图"         1 |  |  |  |
| 时间范围       STEREE        STEREE  | 击"选择部门"来进行选择         选择统计的补丁安装时间范围         选择图表类型,可选择"饼状图"和"横         向柱状图"         1 |  |  |  |

**注意**:补丁安装状态统计和客户端补丁安装状态统计的区别在于前 者是以补丁为关键字,后者是以客户端为关键字来查询。



#### 指定日期内未安装补丁的客户端查询

| 补丁信息查询与统计 |                  |         |
|-----------|------------------|---------|
| 报表类型      | 指定日期内未安装补丁的客户端查询 |         |
| 报表名称      | 指定日期内未安装补丁的客户端查询 |         |
| 所属部门      | 所有部门             | •       |
| 统计的天数     | 10               | 内 0表示不限 |
| 创建状态      | 全局               |         |
| 创建者       | administrator    |         |

| 配置项:      | 说明                                 |
|-----------|------------------------------------|
| 报表类型      | 此报表的类型                             |
| 报表名称      | 此报表的名称                             |
| 所属部门      | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 统计的天数     | 选择要查询的时间点距离今天的天数                   |
| 計丁信息產業与統计 |                                    |

| COMA DUMA COMA |                   |       |                   |  |  |
|----------------|-------------------|-------|-------------------|--|--|
| 17 March 19    | 1.869             | #11b# | MACHIN            |  |  |
| 10.201.22.2    | venus-538c94044   | 而後用   | 00-0c-29-e1-ab-89 |  |  |
| 10.201.33.27   | WIN-QUBBERKIIEQ   | 10年後  | 00-0c-29-0d-7d-83 |  |  |
| 10.201.22.117  | WIN-NEIDITDS96H   | 言葉の   | 00-0c-29-3a-9b-2b |  |  |
| 10.201.100.77  | Jangguan Wei-Angi | notem | 00-00-29-06-13-23 |  |  |

#### 指定日期内客户端补丁安装状态查询

| 补丁信息查询与统计 |                           |
|-----------|---------------------------|
| 祝表类型      | 指定日期内客户端补丁安装状态查询          |
| 报表名称      | 指定日期内客户端补丁安装状态查询          |
| 所属卸门      | 新有部门                      |
| 统计的天数     | 10 内 0表示不限                |
| 创建状态      | 全局                        |
| 创建者       | administrator             |
|           | 保存并执行 保存 执行 <b>删除 取</b> 済 |
| 配置项:      | 说明                        |



|  | 此水的乡   | 此水农的关生                             |   |  |  |  |
|--|--|------------------------------------|---|--|--|--|
| 股表名称   | 此报表的名  | 此报表的名称                             |   |  |  |  |
| 所属部门   | 选择需要查<br>击 <b>"选择</b> 部                        | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |   |  |  |  |
|  |  | 选择要查询的时间点距离今天的天数                   |   |  |  |  |
| 充计的天数<br>  | 选择要查试  | 间的时间点距                             | 离今天的大数  |  |  |  |
| 充计的天数<br>7月25日59日<br>8月10日 8月29日<br>8月11日 8月29日<br>8月11日 8月29日<br>8月11日 8月11日<br>8月11日 8月11日<br>8月111日<br>8月111日 8月111日<br>8月1111<br>8月1111<br>8月1111<br>8月11111<br>8月11111<br>8月11111<br>8月111111<br>8月11111<br>8月11111<br>8月111111<br>8月11111<br>8月11111<br>8月111111<br>8月111111<br>8月111111<br>8月111111<br>8月111111<br>8月111111<br>8月111111<br>8月111111<br>8月111111<br>8月11111111   | 选择要查试  | 间的时间点距<br>2006                     | 离今大的大数  |  |  |  |
| 充计的天数<br><b>     [1828 85 59  </b><br>[1828 85 59  <br>[1828 85 59  | 选择要查试  |                                    | 离今大的大数<br>                                    |  |  |  |
| 充计的天数<br>TESERSSE<br>E2 日期内 8 / 48 / 1<br>E3 / 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1   | 选择要查说<br>····································  |                                    | 离今大的大数<br>——————————————————————————————————— |  |  |  |
| 施计的天数  | 选择要查说<br><del> </del>                          |                                    | 离今大的大数  |  |  |  |
| 施计的天数  | 选择要查说<br>· · · · · · · · · · · · · · · · · · · |                                    | 离今大的大数  |  |  |  |
| 施计的天数<br><b>TESSH555</b><br><b>TESSH555</b><br><b>TESSH555</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b><br><b>TESSH5</b> | 选择要查说<br><del> </del>                          |                                    | 离今大的大数<br>CCTETAT                             |  |  |  |
| 施计的天数<br>(1888年55%)<br>(1888年55%)<br>(1995年1月)(1889年1月)<br>(1995年1月)(1897年1月)<br>(1995年1月)(1897年1月)<br>(1995年1月)(1897年1月)<br>(1995年1月)(1897年1月)<br>(1995年1月)(189777777777777777  | 选择要查说  |                                    | 离今大的大数<br>CCTHEIAT                            |  |  |  |

# 15.5. 审计信息

# 15.5.1. 配置介绍

对文件操作、网站访问、打印,windows 登录,主机名、IP、MAC 变更等进行审计,围绕内网合规管理要求,为内网安全状况持续改 善提供保证。 1



| 计信息查询与统计             |                     |
|----------------------|---------------------|
| 请选择查询统计图表类型 <b>:</b> | ◎ 统计访问次数最多的网站TopN   |
|                      | ◎ 统计访问网站次数最多的电脑TopN |
|                      | ◎ 网站访问审计            |
|                      | ◎ 文件操作审计            |
|                      | ◎ windows登录与注销审计    |
|                      | ◎ 主机名、IP、MAC变更审计    |
|                      | ◎ 打印审计              |
|                      | © windows事件日志查询     |
|                      | ◎ 客户端卸载审计           |
|                      | ◎ windows开关机审计      |
|                      | ◎ 客户端运行审计           |
|                      | ◎ 涉密信息审计查询          |
|                      | ◎ 应用程序运行审计          |
|                      | ◎ FTP审计查询           |
|                      | ◎ 刻录审计              |
|                      | 下一步 取消              |

主机名, IP, MAC 变更审计





| 叶间英国   | 可选择最近更新的天数也可通过点击日期           |  |  |
|--------|------------------------------|--|--|
| 的的短篇   | 图表选择具体时间范围                   |  |  |
| IP 地址  | 输入需要查询的 IP 地址,不填默认查询所<br>有终端 |  |  |
| 主机名    | 输入需要查询的主机名                   |  |  |
| MAC 地址 | 输入需要查询的 MAC 地址               |  |  |

点击 **"执行"** 

| <u>主机名、IP、MAC安要审计</u><br>解放接计 [异出题本] 最为前海 |              |   |                       |   |  |                        |
|---|--------------|---|-----------------------|---|--|------------------------|
| IUMM                                      | Hite         | ai ka   | LENK                  | 夏季南的內容  | 亚里尼的内语   | TTN:                   |
| 172.25.18<br>8.5                          | 2944031<br>E | 10<br>11<br>11<br>11<br>11<br>11<br>11<br>11<br>11<br>11<br>11<br>11<br>11<br>1 | 00-16-25-76-19<br>-5a | ER.6:204031E<br>FF-3140(R) 82505MM<br>Ggabt Network Come<br>don<br>MAC:00-1C-35-7C-19-F<br>A<br>IP-172,25,184,5<br>FF-3140(R) 255 WF-85<br>84 495346<br>MAC:00-1F-38-82-02-8<br>0<br>P1-72,23,188,5 | 主任 8:2944011E<br>同子: Intel(約) 82560MM<br>Gigabit Network Come<br>chan<br>MAC:00-10-25-70-19-F<br>A<br>PHO:000<br>同子: Intel(約) 天然 WHF 経<br>第 49053401<br>MAC:00-15-38-02-02-8<br>9<br>PHO:000 | 2010-7-28 19:0<br>7:59 |

点击 IP 地址链接,进入查看此终端详细信息的界面,即客户端报表。

#### windows 事件日志查询

| 报表类型   | windows事件日志查问 | 1           |        |
|--------|---------------|-------------|--------|
| 报表名称   | windows事件日志查  | <b>I</b> I) | ŢĮ.    |
| 所属部门   | 所有部门          |             | ▼ 选择部门 |
| 时间范围   | ◎最近7          |             |        |
|        | 0 ж           | I 31        |        |
| 事件类型   | 不限            |             |        |
| IP地址范围 | 1             | -           |        |
| 创建状态   | 全局            |             |        |
| 创建者    | administrator |             |        |

| 配置项: | 说明                 |
|------|--------------------|
| 报表类型 | 此报表的类型             |
| 报表名称 | 此报表的名称             |
| 所属部门 | 选择需要查询的终端所属的部门,也可点 |





|         | 击" <b>选择部门"</b> 来进行选择            |
|---------|----------------------------------|
| 时间范围    | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围 |
| 事件类型    | 选择 windows 系统日志中的事件类型            |
| IP 地址范围 | 输入要查询的 IP 地址范围                   |

windows事件目志责资

| 8858 15       | 王四本 亚方自杀       |          |      |  |                     |
|---------------|----------------|----------|------|--|---------------------|
| 17.MM         | 10.00          | 2013/57E | 26   | BIOE   | NH                  |
| 38 201 140 22 | W24-yangweie   |          | 20   | ES SDägent Service 篇<br>유친구 正空泡行 왕종~               | 2012/10/25 15:58:57 |
| 20.201.140.27 | WIN-yangwies   |          | a.e  | Interactive Services De<br>tector 邮件终于 正在运行<br>时在。 | 2012/18/25 13:58-00 |
| 30.201.140.27 | WIN-sangeme    |          | 2.18 | ES Stilgent Service 制<br>条化于 尊正 改正。                | 2012/10/25 16:00:13 |
| 30.201.140.21 | WIN-sangeville |          | 王峰   | 65 IDAgent Senice 新<br>务化于 正常运行 H向。                | 2012/10/25 16:00:25 |
| 30.201.140.27 | WD4-yangeme    |          | 新建   | Windows Error Reports<br>ng Service 解剖社子 正石        | 2012/10/25 16:00:30 |

#### 打印审计



| 配置项:    | 说明                                 |  |  |  |  |  |
|---------|------------------------------------|--|--|--|--|--|
| 报表类型    | 此报表的类型                             |  |  |  |  |  |
| 报表名称    | 此报表的名称                             |  |  |  |  |  |
| 所属部门    | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |  |  |  |  |  |
| 时间范围    | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |  |  |  |  |  |
| IP 地址范围 | 输入要查询的 IP 地址范围                     |  |  |  |  |  |



| TEPHTit<br>Manager (mager               | 1 (2 miles)  |                  |            |         |            |      |                           |
|---|--------------|------------------|------------|---------|------------|------|---------------------------|
| ALL | THE GOVERNME | CONTRACTOR DATE: | 1000000000 | 1000000 | ALCO 10.74 | <br> | Concerning and the second |

#### windows 登录审计

| 报表类型  | windows登录与注销审              | ìt                  |        |
|-------|----------------------------|---------------------|--------|
| 报表名称  | windows登录与注销审              | ĩit                 |        |
| 所属部门  | 所有部门                       |                     | ▼ 选择部门 |
| 时间范围  | ◎ 最近 <mark>7</mark><br>◎ 从 | 天<br>回 <sub>到</sub> |        |
| P地址范围 |                            | -                   |        |
| 刘建状态  | 全局                         |                     |        |
| 创建者   | jing                       |                     |        |

| 配置项:    | 说明  |
|---------|---|
| 报表类型    | 此报表的类型                                      |
| 报表名称    | 此报表的名称                                      |
| 所属部门    | 选择需要查询的终端所属的部门,也可点<br>击 <b>"选择部门"</b> 来进行选择 |
| 时间范围    | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围            |
| IP 地址范围 | 输入要查询的 IP 地址范围                              |

| windows 日<br>放出出来 | COLUMN RAN | 18   |     |     |          |            |
|-------------------|------------|------|-----|-----|----------|------------|
| 371614            | 010100     | 1105 | 185 | MAR | 82       | REAL       |
| 1.                |            |      |     |     | <b>1</b> | 四/共有100分数据 |

文件操作审计





| 配置项:             | 说明  |
|------------------|---|
| 报表类型             | 此报表的类型                                      |
| 报表名称             | 此报表的名称                                      |
| 所属部门             | 选择需要查询的终端所属的部门,也可点<br>击 <b>"选择部门"</b> 来进行选择 |
| 时间范围             | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围            |
| IP 地址范围          | 输入要查询的 IP 地址范围                              |
| 文件审计筛选           | 选择文件操作的种类,如创建、修改、删<br>除等                    |
| <b>半社供報度和与核社</b> |   |

| 文件解                   | 2.任 <u>操作取住</u><br>835年8月 - 写四题条 使为尚是 |                 |   |  |          |   |     |                         |                             |
|-----------------------|---------------------------------------|-----------------|---|--|----------|---|-----|-------------------------|-----------------------------|
| arritat.              | 12                                    |                 | #205  | ANTON  | B        | 21  |     | 80.0.I                  | 4111                        |
| 1 <u>883</u>          | Buye<br>an-P<br>C                     | <del>4</del> 1е | C/Elsers/Juscum/AppD<br>ata/Reaming/Microsoft/<br>Inter/IHIC/T/PLeamLDA<br>T  | C:\UserViewwariyopD<br>ataiRoaningWicrosoft)<br>IntelMICC/PLearnE.DA<br>T  |          | CriProgram Files (5861)<br>Tencent/QQ/Bin/QQ.ax<br>B  | W.  | 255.25<br>5.255.2<br>55 | 2012/1<br>0/31 1<br>5:23:11 |
| 10.20<br>10.00<br>10  | ikiyu<br>an‡<br>C                     | 猳               | C:Nosers'skivusni AppD<br>atsUbarring/Microsoft/<br>Ime/JHSCSIPLearnS.0A<br>T   | C:WsersikuwaniAppD<br>ataiApamingPicrosoft,<br>bneUMSCSVPLearinS-DA<br>T   | 8        | C1/Program Files (x86)\<br>Tencent()QQ/dim(QQ.ex<br>e | īγ. | 255-25<br>5-255-2<br>55 | 2012/1<br>1/31 1<br>5:23:11 |
| 10,20                 | ikayu<br>an-P<br>C                    | eje             | C. Waterrickey-carri-AppD<br>atayLocal Vecroeoff Own<br>dews Velatory Velatory. IE<br>Byelinero 130 1210312<br>0121101 Vedex. dat | C:WoerviewschippD<br>ataraccal/Microsoft/Wie<br>dowa/History/History/R<br>Synthiato1201210313<br>0121101/jndex.dat | 20       | C:\Program Files (x86)\<br>Tencent\QQ'BimQQ ex<br>9   | w   | 255.25<br>5.255.2<br>55 | 2012/1<br>3/31 1<br>5:23:11 |
| 10.20<br>1 00.2<br>13 | and<br>C                              | η.              | C-Riters'deviceriAppD<br>ata/Acaming/Vectoroff)<br>Ime/JMSCS/PLearnL84<br>T   | C:WsersikosuariAppD<br>ata/kuaring/Honsoft/<br>Ime/IMSCS/PLearnLDA<br>T  | #<br>\$1 | C:\Program Files (x86)\<br>Tencent\QQ\Bin\QQ.mr<br>e  | W.  | 255.25<br>3.295.7<br>55 | 2012/1<br>0/31 1<br>4:58:29 |

网站访问审计





| 配置项:     | 说明                                 |
|----------|------------------------------------|
| 报表类型     | 此报表的类型                             |
| 报表名称     | 此报表的名称                             |
| 所属部门     | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 主机名      | 输入要查询的主机名                          |
| 时间范围     | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| IP 地址范围  | 输入要查询的 IP 地址范围                     |
| 网站审计是否允许 | 选择是否允许网站审计的条件                      |

| STORE &     | 王机在树             | 副目的部        | HRMM               | 相称                  |
|-------------|------------------|-------------|--------------------|---------------------|
| 10 291 33.2 | verxel-518c94044 | 二個6         | www.sitis.com.cn/  | 2012/10/30 15:30:29 |
| 10.201.33.2 | vanus-518c94044  | 268         | www.sitta.com.ctv/ | 2012/10/38 15:30:28 |
| 55,221,33.2 | vmvm-518c94044   | 288         | www.sitss.com.ctu  | 2812/10/38 13:30:27 |
| 10 201 33.2 | vinus-518c94044  | 2.69        | www.arsa.com.cn/   | 3012/10/38 LB:30:27 |
| 10 201 33.2 | verser-518:94044 | 289         | www.sina.com.cn/   | 2012/10/30 15:30:27 |
| 10 201 33 2 | venus-518c94044  | <u>_68</u>  | www.sina.com.cn/   | 3012/10/30 15:30:27 |
| 20.201.33.2 | verus-518c94044  | 288         | www.sina.com.cn/   | 2012/10/30 15:30:27 |
| 10.201.33.2 | versal-516c94044 | 200         | www.seta.com.cn/   | 3012/10/30 15:50:27 |
| 10.201.33.2 | verse-319c94044  | 280         | www.sitis.com.tn/  | 2012/10/28 15:30:27 |
| 20 201 33.2 | versus-518:94044 | <b>_100</b> | www.sitia.com.m/   | 2012/10/38 15:30:27 |

统计访问次数最多的电脑 Top10





| 报表类型  | 续计访问网站次数最多(              | 的电脑TopN  |                          |
|-------|--------------------------|----------|--------------------------|
| 报表名称  | 统计访问同志次数最多               | 的电脑TopN  |                          |
| 新麗部门  | 新有部门                     |          | <ul> <li>法提供门</li> </ul> |
| HATE  | ● 最近 7<br>〇 从            | *<br>• 9 | E                        |
| TopN  | 10                       |          |                          |
| 图表类型  | ● 天图<br>○ 排状图<br>○ 編句性状態 |          |                          |
| 的建状态  | 全局                       |          |                          |
| BRIZM | jing                     |          |                          |

| 配置项:  | 说明  |
|---|---|
| 报表类型  | 此报表的类型                                      |
| 报表名称  | 此报表的名称                                      |
| 所属部门  | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择          |
| 时间范围  | 选择统计时间范围                                    |
| TOPN  | 输入要统计的最大终端数                                 |
| 图表类型  | 选择图表类型,可选择"饼状图"和"横<br>向柱状图"                 |
| #建築創度群均開設<br>然計畫同次 微量 多的 电描 Tup 10<br>編曲時計 第22回表 在为用品<br>12月11 美工業21<br>1 | ■138年 14年2月<br>■15月2日年<br>■15月2日年1月1日年1月1日日 |

统计访问次数最多的网站 Top10





| 配置项: | 说明                                   |
|------|--------------------------------------|
| 报表类型 | 此报表的类型                               |
| 报表名称 | 此报表的名称                               |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择   |
| 时间范围 | 选择统计时间范围                             |
| TOPN | 输入要统计的最大终端数                          |
| 图表类型 | 选择图表类型,可选择 <b>"饼状图"</b> 和"横<br>向柱状图" |

| HAL                        | 6-17.D       |
|----------------------------|--------------|
| www.soso.com               | 58           |
| tim/ya.cn                  | 20           |
| www.ttansis.cn             | 24           |
| fownland.windowsupdate.com | 29           |
| man ailyee.com             | 42           |
| mastercorm.gg.com          | 12           |
| ggshew2-kem.gg.com         | 14           |
| static tiony aut com       | 12           |
| www.sina.cim.on            | 52           |
| agshow2-item.ag.com/       | 10           |
| *                          | 重1四/林甸1四10条数 |

客户端卸载审计





| 配置项:    | 说明                                 |
|---------|------------------------------------|
| 报表类型    | 此报表的类型                             |
| 报表名称    | 此报表的名称                             |
| 所属部门    | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围    | 选择查询的时间范围                          |
| IP 地址范围 | 选择查询的 IP 范围                        |

| 3户端卸载审计<br>3334表 异出图表 | 设为首选            |      |       |                    |
|-----------------------|-----------------|------|-------|--------------------|
| Pitt                  | 主机名称            | 副门名権 | 事件内容  | 上編制員               |
| 10.201.222.65         | admin-774c3efd9 |      | 卸動客户端 | 2011/9/14 9:46:14  |
| 10.201.99.23          | jian-win2K3X64  | с    | 卸载客户端 | 2011/9/14 10:07:30 |

#### windows 开关机审计









| 风险管理与审计系统 V6.6.9.4 | 4Patch66940000 用户手册                |
|--------------------|------------------------------------|
|                    |                                    |
| 报表类型               | 此报表的类型                             |
| 报表名称               | 此报表的名称                             |
| 所属部门               | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围               | 选择查询的时间范围                          |
| IP 地址范围            | 选择查询的 IP 范围                        |

| 4       | TT 12 HI (\$2.11) |
|---------|-------------------|
| #1000#D | 在大街里14            |
|         |                   |

| 核政振為 导出的      | A CONTRACTOR  |                 |            |     |                    |
|---------------|---------------|-----------------|------------|-----|--------------------|
| IPIRM.        | 2028 B25      | 18.6            | 加加市        | 2.5 | 111                |
| 10.201.20.21  |               | WIN-HACLF04CSLU |            | 开机  | 2011/9/14 13:25:24 |
| 10.201.20.21  |               | WIN-HACLF04CSLU |            | 邗机  | 2011/9/14 13:31:12 |
| 10.201.20.21  | Administrator | WIN-HACLF04C5LU |            | 邢帆  | 2011/9/14 14:01:45 |
| 10.201.20.21  |               | WIN-HACLF04CSLU |            | 开机  | 2011/9/14 14:08:41 |
| 10.201.88.3   |               | 间放红             | darren.com | 关机  | 2011/9/14 14:34:45 |
| 10.201.88.3   |               | 间底红             | darren.zom | 肝机  | 2011/9/14 14:39:12 |
| 10.201.222.20 |               | WIN-SEVLARPS6OC |            | 开机  | 2011/9/13 23:46:13 |
| 10.201.222.65 |               | WIN-zsdzsd      |            | 开机  | 2011/9/14 15:03:20 |
| 10.201.222.66 | Administrator | ADMIN-774C3EED9 |            | ₩ł, | 2011/9/14 15:03:26 |
| 10.201,222.20 |               | WIN-9EVL8RP96OC |            | 邗机  | 2011/9/14 0:03:32  |
| BE 1234567    | 8910          |                 |            |     | 第2页/共有24页237条数据    |

#### 客户端运行审计





| 时间范围    | 选择查询的时间范围   |
|---------|-------------|
| IP 地址范围 | 选择查询的 IP 范围 |

| 审计信息查询与统计<br><u>客户端运行</u> 审计<br> |                                   |      |               |         |      |                     |
|----------------------------------|-----------------------------------|------|---------------|---------|------|---------------------|
| 191616                           | 主机轰炸                              | 銀口名作 | windows用户名    | 能搬系统用户名 | 重件类型 | RLAT                |
| 10.201,140.1                     | admin-yangweie                    | 二銀8  | administrator |         | 更新第副 | 2012/10/25 15:48:41 |
| 10,201,140,27                    | WIN-yangweie                      | 二根A  | Administrator |         | 更新策略 | 2012/10/25 15:48:02 |
| MA 10 82 83 84                   | <u>85 86 87 88 89 90 <b>9</b></u> | 1 末直 |               |         |      | 第91页/共有91页902条数据    |

#### 涉密信息审计查询



| 配置项: | 说明                                 |
|------|------------------------------------|
| 报表类型 | 此报表的类型                             |
| 报表名称 | 此报表的名称                             |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 主机名  | 输入需要查询的主机名                         |
| 时间范围 | 选择查询的时间范围                          |



| IP 地址范围               |               | 选择查询的 IP 范围           |   |         |  |  |
|-----------------------|---------------|-----------------------|---|---------|--|--|
| 涉密关键字                 |               | 输入在                   | 查询的关键字  | ,多关     | 关键字以/分隔                                  |  |
| ●日前息素用加除社<br>送完信息市计查计 |               | -                     |   |         |  |  |
| REAL TO BE            | ALE REAL REAL | 0111506               | 文月長台  | KA 8.00 | 1.807.03                                 |  |
| 10 301 90 203         | I DIM IAN-PC  | and the second second | Contraction of the second s | 107.4   |  |  |
|                       | - carrower c  |                       | C:頃戸/kuvau/虚重/DNS<br>違入女威改進戦要役计3.do<br>に  | MIL     | 2011/9/26 15:12:25                       |  |
| 10.201.00.202         | LIUMAN-PC     |                       | C·(利州Auvau)建築/DNS<br>進入市場改造教養後計3.do<br>E<br>C·(Program Films (JBB))<br>WinRARS/License.fxt                      | Rift.   | 2011/9/26 15:12:25<br>2011/9/26 15:12:25 |  |

#### FTP 审计查询



| 配置项:    | 说明  |
|---------|---|
| 报表类型    | 此报表的类型                                      |
| 报表名称    | 此报表的名称                                      |
| 所属部门    | 选择需要查询的终端所属的部门,也可点<br>击" <b>选择部门"</b> 来进行选择 |
| 时间范围    | 选择查询的时间范围                                   |
| IP 地址范围 | 选择查询的 IP 范围                                 |
| 传输文件名称  | 选择查询的 FTP 文件名                               |
| 操作类型    |   |



| ADDRA DUDRA       |               |                       |                          |
|-------------------|---------------|-----------------------|--------------------------|
| new LRSS          | #136.W        | 179%新建地址 疑念 机构文件名称    |                          |
|                   |               |                       | 第3回/共有1回日告告请             |
| 刻录审计              |               |                       |                          |
| 报表类型<br>报表名称      | 封录审计          |                       |                          |
| 所罵部门              | 所有部门          |                       | <ul> <li>送择部门</li> </ul> |
| 时间范围              | ● 最近 7<br>○ 从 | 天<br>団 到              |                          |
| IP地址范围            |               |                       |                          |
| 源义[F-名称<br>目标文件名称 |               |                       |                          |
| 创建状态              | 全局            |                       |                          |
| 创建者               | jing          |                       |                          |
|                   | 保存并执          | 行 保存 执行 取消            |                          |
| 配置项:              |               | 说明                    |                          |
| 报表类型              |               | 此报表的类型                |                          |
| 报表名称              |               | 此报表的名称                |                          |
| 庇屋如门              |               | 选择需要查询的终端所属的部         | 邓门,也可点                   |
| 1 (年時)            |               | 击" <b>选择部门"</b> 来进行选择 |                          |
| 时间范围              |               | 选择查询的时间范围             |                          |
| IP 地址范围           |               | 选择查询的 IP 范围           |                          |
| 源文件名称             |               | 选择查询的刻录源文件名称          |                          |
| 目标文件名称            |               | 选择查询的刻录的目标文件名         | <b>7</b><br>]            |

#### 应用程序运行审计



| 报表类型                                 | 应用程序运行           | 审计       |                         |                         |               |                         |
|--------------------------------------|------------------|----------|-------------------------|-------------------------|---------------|-------------------------|
| 报表名称                                 |                  |          |                         |                         |               |                         |
| 新属部门                                 | 新物部门             |          |                         |                         |               | 法保護门                    |
| 时间后期                                 | HIPPOPI J        |          | -                       |                         |               |                         |
|                                      | O M              |          |                         | Ú.                      |               | <b>H</b>                |
| IP地址范围                               |                  |          |                         | -213                    |               |                         |
| 创建状态                                 | 全局               |          |                         |                         |               |                         |
| 创建者                                  | jing             |          |                         |                         |               |                         |
|                                      | 保存并执行            | ti 🗌     | 保存 1                    | 机行 1                    | 能消            |                         |
| 町里 西                                 | 1                | 计四       |                         |                         |               |                         |
| <b></b> 能直坝:                         |                  | 况明       |                         |                         |               |                         |
| 报表类型                                 |                  | 此报       | 表的类型                    |                         |               |                         |
| 报表名称                                 |                  | 此报       | 表的名称                    |                         |               |                         |
| 所属部门                                 |                  | 选择<br>击" | 需要查询的<br><b>选择部门"</b>   | 」终端所属<br>来进行选           | 的部Ì<br>择      | ],也可点                   |
| 时间范围                                 |                  | 选择       | 查询的时间                   | ]范围                     |               |                         |
| IP 地址范围                              |                  | 选择       | 查询的 IP 氵                | 范围                      |               |                         |
| 应用程序运行审计<br>60.8%本 <sup>Morest</sup> | a                |          |                         |                         |               |                         |
| 1780 1589                            | DE AREN          |          | 102104                  | 81211A                  | 15.611<br>11月 | LINE                    |
| 10 201 90.2 Sayes                    | -S dhost.ese     | 5        | 2012/30/28 14:0<br>8:25 | 2012/10/26 14:0<br>8:33 | -             | 2012/10/26 14:0         |
| 10.201.90.2 Bayean-                  | -III inabsync.ex | 06       | 2012/10/26 14:0         | 3812/10/26 14:0         | 5902          | 2012/10/26 14:1         |
| 10.201.99.2 Novem-                   | -8 dihost.exe    |          | 2012/30/28 14:1<br>0:25 | 2012/30/26 14:3         | 1.369         | 2012/10/26 14:1<br>1:45 |
| 10.201.00.2 Baysan-                  | -III worfault.co | 0        | 2012/30/26 14:1<br>0:40 | 3012/30/26 14:3<br>0:58 | 989           | 2012/10/26 14:1<br>2:46 |
| 10.201.80.2 haven                    | -0 dhost.exe     |          | 2012/10/26 14:1         | 2012/10/26 14:1         | 78            | 2012/10/26 14:1         |
| 10.201.90.2 Royan                    | -fil sychost.com |          | 2012/30/26 14:0<br>9:27 | 2012/10/26 14:1<br>2:58 | 2014122       | 2012/10/26 14:1<br>4:47 |
| 10.201.90.2 Royum                    | -0 dhost.ext     |          | 2012/20/26 14:1         | 2012/10/26 14:1         | 50            | 2012/18/26 14:1         |
| 10.201.90.2 Raysan                   | -ill ditost.ers  |          | 2012/10/26 14:1         | 2012/10/26 14:1<br>3:23 | 469           | 2012/18/26 14:1<br>4:47 |
| 10.201 90.2 kayust                   | -@ dhost.exe     |          | 2012/10/28 14:1<br>3:20 | 2012/10/26 14:1         | 88            | 2013/10/26 14:1<br>4:47 |
| 10.201.90.2 luyuan                   |                  | host.eve | 2012/30/26 14:1         | 2012/10/26 14:1         | 1599-49       | 2012/10/26 14:1         |

# 15.6. 安全基线

単元12312028210…主元

## 15.6.1. 配置介绍

受控终端安全基线状态和历史记录,包括进程违规,软件安装违规, 病毒码违规,强制补丁违规,安全加固等。

重1页/共有28页273单数集



| 安全基线查询与统计    |                     |
|--------------|---------------------|
| 请选择查询统计图表类型: | ◎ 终端安全基线讳规TopN      |
|              | ◎ 进程违规状态查询          |
|              | ◎ 强制补丁违规状态查询        |
|              | ◎ 病毒码违规状态查询         |
|              | ◎ 安全加固-加入和登录域统计     |
|              | ◎ 安全加固-域策略违规状态查询    |
|              | ◎ 软件安装违规状态查询        |
|              | ◎ 进程违规历史查询          |
|              | ◎ 强制补丁违规历史查询        |
|              | ◎ 病毒码违规历史查询         |
|              | ◎ 安全加固-域策略违规历史查询    |
|              | ◎ 软件安装违规历史查询        |
|              | 🔘 计算机帐号查询           |
|              | ◎ ServicePack违规状态查询 |
|              | ◎ ServicePack违规历史查询 |
|              | ◎ 终端共享资源查询          |
|              | 下一步 取消              |



| 安全基线查询与统计    |                      |
|--------------|----------------------|
|              |                      |
| 请选择查询统计图表类型: | ◎ 终端安全基线违规TopN       |
|              | 🖗 进程违规状态查询           |
|              | ◎ 强制补丁违规状态查询         |
|              | ◎ 病毒码违规状态查询          |
|              | 😳 安全加固-自定义安全策略违规状态查询 |
|              | 💿 安全加固-加入和登录域统计      |
|              | 🖗 安全加固-城策略违规状态查询     |
|              | ◎ 软件安装违规状态查询         |
|              | ◎ 进程违规历史查询           |
|              | ◎ 强制补丁违规历史查询         |
|              | ◎ 病毒码违规历史查询          |
|              | 🖗 安全加固-自定义安全策略违规历史查询 |
|              | ◎ 安全加固-城策略违规历史查询     |
|              | 问 软件安装违规历史查询         |
|              | 🗇 计算机帐号查询            |
|              | ◎ ServicePack违规状态查询  |
|              | ◎ ServicePack违规历史查询  |
|              | ◎ 终端共享资源控制和管理        |
|              | 下一步 取消               |





| 配置项: | 说明     |
|------|--------|
| 查询类型 | 此查询的类型 |



| 查询名称 | 此查询的名称                               |
|------|--------------------------------------|
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择   |
| 时间范围 | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围     |
| TOPN | 输入需要查询出的统计最大数量                       |
| 图表类型 | 选择图表类型,可选择" <b>饼状图"</b> 和"横<br>向柱状图" |

#### 点击执行

| 修建安全草铁击铁T。<br>维查服务 导出用表 住 | 10<br>58.4     |              |              |
|---------------------------|----------------|--------------|--------------|
| IPRE                      | 18.28          | 30364        | <b>由田次</b> 章 |
| 18.201.140.1              | admin sangeeia | <b>未知能()</b> | 172          |
| 1                         |                |              | 第1页/共有1页1条的# |

#### 红名单进程违规历史查询

| 採表类型         | 进程违规历史查询            |     |           |     |      |
|--------------|---------------------|-----|-----------|-----|------|
| 报表名称         | 红名单进程违规因            | 史查词 |           |     |      |
| 宣调条件         | 红名单                 |     |           | -   |      |
| 所實部门         | 所有部门                |     |           |     | 选择部门 |
| 时间范围         | ● 最近 7<br>○ 从       |     | 天<br>回 )) |     | 3    |
| 操作系统<br>IP地址 | 不穩定                 |     |           | •   |      |
| 主机名          |                     |     |           |     |      |
| 创建状态<br>创建者  | 全局<br>administrator |     |           |     |      |
|              | 保存并执行               | 保存  | 执行        | 902 | Dă   |

| 配置项: | 说明                                 |
|------|------------------------------------|
| 报表类型 | 此查询的类型                             |
| 报表名称 | 此查询的名称                             |
| 查询条件 | 选择进程查询类型                           |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |



| 时间范围  | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围 |
|-------|----------------------------------|
| 操作系统  | 选择操作系统                           |
| IP 地址 | 输入要查询的 IP 地址                     |
| 主机名   | 输入要查询的主机名                        |

#### 红名单进程违规历史查询

| 然改振击         | 导出题表 设         | 为首选    |                   |                           |            |                     |
|--------------|----------------|--------|-------------------|---------------------------|------------|---------------------|
| IFIEM        | LKAR           | 101103 | mochele           | <u>维乐条</u> 师              | 成介示统       | LINK                |
| 10.201.140.1 | admin-yangweie | -48    | 00-0C-29-16-8E-34 | cmd.exe                   | Windows XP | 2012/10/25 16:54:53 |
| 10.201.140.1 | admin-yangweie | -10    | 00-0C-29-16-8E-34 | cmd.exe                   | Windows XP | 2012/10/25 17:05:54 |
| 10.201.140.1 | admin-yangweis |        | 00-0C-29-16-8E-34 | cmd.axe                   | Windows XP | 2012/10/25 17:05:54 |
| 10:201 140.1 | admin-yangweie | -10    | 00-0C-29-16-8E-34 | cmd.exe                   | Windows XP | 2012/10/25 17:07:56 |
| 10,201,140,1 | admin-yangweie | -40    | 00-0C-29-16-8E-34 | cmd.exe                   | Windows XP | 2012/10/25 17:45:04 |
| 10.201.140.1 | admin-yangweie | -10    | 00-0C-29-16-8E-34 | 文件审计与目录加密地结查<br>用明试工具-exe | Windows XP | 2012/10/25 17:45:04 |
| 10.201.140.1 | admin-yangweie | 101    | 00-0C-29-16-8E-34 | cmd.exe                   | Windows XP | 2012/10/25 17:46:05 |
| 10.201.140.1 | admin-yangweie | -18    | 00-0C-29-16-8E-34 | 文件审计与目录加密编动考<br>用则试工具_exe | Windows XP | 2012/10/25 17:46:05 |
| 10.201 140.1 | admin-yangweie |        | 00-0C-29-16-8E-34 | cmd.exe                   | Windows XP | 2012/10/25 17:47:05 |
| 10,201,140.1 | admin-yangweie | -48    | 00-0C-29-16-8E-34 | 文件审计与目录加密提动者<br>用则试工具_exe | Windows XP | 2012/10/25 17:47:05 |
| M版12 图页      |                |        |                   |                           |            | 第1页/共有2页13条数据       |

#### 红名单进程违规状态查询





|                     | 击" <b>选择部门"</b> 来进行选择            |  |  |
|---------------------|----------------------------------|--|--|
| 时间范围                | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围 |  |  |
| 操作系统                | 选择操作系统                           |  |  |
| IP 地址               | 输入要查询的 IP 地址                     |  |  |
| 主机名                 | 输入要查询的主机名                        |  |  |
| 1.5.0.000 COME COME |                                  |  |  |

#### 黑名单进程违规状态查询



| 配置项: | 说明                                 |
|------|------------------------------------|
| 报表类型 | 此查询的类型                             |
| 报表名称 | 此查询的名称                             |
| 查询条件 | 选择进程查询类型                           |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围 | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| 操作系统 | 选择操作系统                             |



| IP 地址  | 输入要查询的 IP 地址 |              |      |             |  |  |
|--|--------------|--------------|------|-------------|--|--|
| 主机名  | 输入要查         | 询的主机         | 名    |             |  |  |
| 第二日本<br>第二日本<br>第二日本<br>第二日本<br>第二日本<br>第二日本<br>第二日本<br>第二日本 | machille     | <b>在</b> 开西市 | 潮作系列 | 1.980.00    |  |  |
| 1  |              |              |      | 第1页出来1页2条曲框 |  |  |

### 白名单进程违规状态查询

| 安全基线查询与统计 |               |       |          |
|-----------|---------------|-------|----------|
| 报表类型      | 进程违规状态查询      |       |          |
| 报表名称      | 白名單进程書規状态查    | а́    |          |
| 重调条件      | 白名単           |       | <br>e e  |
| 所國部门      | 所有部门          |       | <br>选择部门 |
| 时间范围      | ● 最近 7        | Ŧ     | 0.03     |
|           | O M           | II 카  |          |
| 播作系统      | 不穩定           |       | <br>ē.   |
| 印绝址       |               |       |          |
| 主机名       |               |       |          |
| 创建状态      | 全局            |       |          |
| 包藏者       | administrator |       |          |
|           | 保存并执行         | 保存 执行 | <br>取消   |

| 配置项:  | 说明                                 |
|-------|------------------------------------|
| 报表类型  | 此查询的类型                             |
| 报表名称  | 此查询的名称                             |
| 查询条件  | 选择进程查询类型                           |
| 所属部门  | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围  | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| 操作系统  | 选择操作系统                             |
| IP 地址 | 输入要查询的 IP 地址                       |
| 主机名   | 输入要查询的主机名                          |



| 白名単計目<br>和改革素 | (法規状法由)<br>(10000年 | 2,540,8 |          |       |      |              |
|---------------|--------------------|---------|----------|-------|------|--------------|
| INCOM         | THE                | 10110-0 | mar Mile | 6.528 | 化化成物 | 1.8004       |
| 3             |                    |         |          |       |      | 第1页/共有1页0条焦焊 |

### 强制补丁违规状态查询

| 探表类型         | 强制补丁违规状态查询                    |        |
|--------------|-------------------------------|--------|
| 报表名称         | 僅創計丁連規状态宣审                    | 1      |
| 所實部门         | 所有部门                          | • 选择部门 |
| 时间范围         | ● 截近7 <del>天</del><br>○ 从 □ 到 |        |
| 操作系统         | 不指定                           | •      |
| IP地址         |                               |        |
| 主机名          | -                             |        |
| 创建状态         | 主局                            |        |
| 092 <b>4</b> | administrator                 |        |

| 配置项:   | 说明                                     |  |  |  |  |  |
|--|--|--|--|--|--|--|
| 报表类型   | 此查询的类型                                 |  |  |  |  |  |
| 报表名称   | 此查询的名称                                 |  |  |  |  |  |
| 所属部门   | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择     |  |  |  |  |  |
| 时间范围   | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围       |  |  |  |  |  |
| 操作系统   | 选择操作系统                                 |  |  |  |  |  |
| IP 地址  | 输入要查询的 IP 地址                           |  |  |  |  |  |
| 主机名  | 输入要查询的主机名                              |  |  |  |  |  |
| 田村谷丁市現状态会自<br>和か年期 日本期表 日本期表<br>1012年 上秋秋 は11月日<br>1 | metting 计工程机 建石基线 上的时间<br>第15月2日170日日期 |  |  |  |  |  |

病毒码违规状态查询



第1页/共有1页1条数据

| 报表类型                              | 病毒码违规协                  | 态查询              |                     |                        |               |          |
|-----------------------------------|-------------------------|------------------|---------------------|------------------------|---------------|----------|
| 报表名称                              | 病毒码违规制                  | 状态查询             |                     |                        |               |          |
| 所属部门                              | 所有部门                    |                  |                     |                        |               | ▼ 选择部门   |
| 时间范围                              | ④ 最近 7                  |                  |                     | 天                      |               |          |
|                                   | © ∦                     |                  |                     | 1 到                    |               |          |
| 操作系统                              | 不指定                     |                  |                     |                        |               | •        |
| IP地址                              |                         |                  |                     |                        |               |          |
| 主机名                               |                         |                  |                     |                        |               |          |
| 创建状态                              | 全局                      |                  |                     |                        |               |          |
| 创建者                               | administrat             | or               |                     |                        |               |          |
|                                   | 保存并执行                   | Ī                | 保存                  | 执行                     | 删除            | 取消       |
| 配置项:                              |                         | 说明               |                     |                        |               |          |
| 报表类型                              |                         | 此查               | 询的类                 | 型                      |               |          |
| 报表名称                              |                         | 此查               | 询的名                 | 称                      |               |          |
| 所属部门                              |                         | 选择<br>击 <b>"</b> | 需要查<br>" <b>选择部</b> | 词的终端<br>【 <b>门"</b> 来注 | 端所属的部<br>进行选择 | 3门,也可点   |
| 时间范围                              |                         | 可选图表             | 译最近<br>选择具          | 更新的<br>。<br>体时间 彩      | 天数也可通<br>范围   | i过点击日期   |
| 操作系统                              |                         | 选择               | 操作系                 | 统                      |               |          |
| IP 地址                             |                         | 输入               | 要查询                 | 的 IP 地                 | 址             |          |
| 主机名                               |                         | 输入               | 要查询                 | 的主机                    | 名             |          |
| 病素約注現状态素約<br>低かなあ<br>10.2011年32 W | SARA<br>R.C. I<br>N-ywe | E16M             | RARAS               | 10 <b>9-01</b> 211-    | 2012/11/1     | 10:41:04 |

安全加固-加入和登录域统计

1



| 报表类型 | 安全加固-加入和登录域统计                           | ł        |        |
|------|---|----------|--------|
| 报表名称 | 安全加固-加入和登录域统计                           | ł        |        |
| 所属部门 | 所有部门                                    |          | ▼ 选择部门 |
| 时间范围 | <ul> <li>● 最近 7</li> <li>● 从</li> </ul> | 天<br>回 到 |        |
| 图表类型 | ◎ 无图                                    |          |        |
|      | ◎ 饼状图                                   |          |        |
|      | ◎ 横向柱状图                                 |          |        |
| 创建状态 | 全局                                      |          |        |
| 创建者  | administrator                           |          |        |
|      | 保存并执行保存                                 | 穿 执行     | 删除 取消  |

| 配置项: | 说明                                 |
|------|------------------------------------|
| 报表类型 | 此查询的类型                             |
| 报表名称 | 此查询的名称                             |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围 | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| 图表类型 | 选择图表类型,可选择"饼状图"和"横<br>向柱状图"        |

| AMERICAN          | 126A  |              |
|-------------------|---|--------------|
| x3\266            | 22  |              |
| λ <del>Ξ0</del> 5 | 4   |              |
| 7965              | 9   |              |
|                   |   | 10/1410398   |
|                   | <ul> <li>正知入事報報</li> <li>加入事報報</li> <li>加入事報報</li> <li>登录牙利報</li> </ul> | 32<br>4<br>0 |
|                   | 白井  | 36           |
|                   |   |              |
|                   |   |              |
|                   |   |              |

安全加固-域策略违规状态查询



| 报表类型 安全加固-域策略违规状态查询 |   |                                    |  |  |  |  |
|---------------------|---|------------------------------------|--|--|--|--|
| 报表名称                | 安全加固-域                                  | 演蹈违规状态查询                           |  |  |  |  |
| 所属部门                | 所有部门                                    | ▼ 送释部门                             |  |  |  |  |
| 时间范围                | <ul> <li>● 最近 7</li> <li>○ ц</li> </ul> |                                    |  |  |  |  |
| 操作系统                | 不指定                                     |                                    |  |  |  |  |
| IP地址                |   |                                    |  |  |  |  |
| 主机名                 |   |                                    |  |  |  |  |
| 创建状态                | 全局                                      |                                    |  |  |  |  |
| 创建者                 | administra                              | tor                                |  |  |  |  |
|                     | 保存并执行                                   | 行                                  |  |  |  |  |
| 配置项:                |   | 说明                                 |  |  |  |  |
| 报表类型                |   | 此查询的类型                             |  |  |  |  |
| 报表名称                |   | 此查询的名称                             |  |  |  |  |
| 所属部门                |   | 选择需要查询的终端所属的部门,也可点<br>击"洗择部门"来进行选择 |  |  |  |  |
|                     |   |                                    |  |  |  |  |

| 安全加强-<br> | CHARLER R | <u>秋杰弗尚</u><br> |                |                |              |
|-----------|-----------|-----------------|----------------|----------------|--------------|
| IPRE      | INC       | <b>BELLER</b>   | ANALSER STREET | <b>B</b> 0.5.1 | Linite       |
| 3         |           |                 |                |                | NIGORAL BORN |

图表选择具体时间范围

输入要查询的 IP 地址

输入要查询的主机名

选择操作系统

可选择最近更新的天数也可通过点击日期

白名单软件安装违规状态查询

时间范围

操作系统

IP 地址

主机名





| ктны  |                                    |
|-------|------------------------------------|
| 配置项:  | 说明                                 |
| 报表类型  | 此查询的类型                             |
| 报表名称  | 此查询的名称                             |
| 所属部门  | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 查询条件  | 选择进程查询条件                           |
| 时间范围  | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| 操作系统  | 选择操作系统                             |
| IP 地址 | 输入要查询的 IP 地址                       |
| 主机名   | 输入要查询的主机名                          |

| 白名単软件                 | 安装违规实           | 志改治            |
|-----------------------|-----------------|----------------|
| and the second second | And shares in a | C. Drate Model |

| 18.8    | OD BAR                                   | W.IS-ALW  | <b>除住.</b> 所用  | 1.8404  |
|---------|--|---|--|---|
| W3N-ywe | - mi                                     | MORETT  | Windows 7  | 2012/11/1 10:41:44  |
| W2N-ywa | mj                                       | QQPvoted  | Windows 7  | 2012/11/1 10:41:44  |
| WZEYWE  | mj                                       | QQ软件管理1.0 Reta3   | Windows 7  | 2012/11/1 10:41:44  |
| WIR-ywa | mj                                       | 他们QQ2012(世纪的时)  | Windows 7  | 2012/11/1 10:41:44  |
|         | W29-ywe<br>W29-ywe<br>W29-ywe<br>W29-ywe | A.N.A.         0211-04           W39-ywe         mp           W39-ywe         mp           W39-ywe         mp           W39-ywe         mp           W39-ywe         mp | L.N.C.         W112.00         W112.00           W30-ywe         mp         360@9211           W30-ywe         mp         QQProtect           W30-ywe         mp         QQR(H10000012000000000000000000000000000000 | LTLD         IV1220         IV1220         IV1220           W3H-ywe         mp         360%±21         Windows 7           W3H-ywe         mp         QQProtect         Windows 7           W3H-ywe         mp         QQProtect         Windows 7           W3H-ywe         mp         QQR(1120)         Windows 7           W3H-ywe         mp         Mindows 7         Windows 7           W3H-ywe         mp         Mindows 7         Windows 7 |

黑名单软件安装违规状态查询





| 配置项:  | 说明                                 |
|-------|------------------------------------|
| 报表类型  | 此查询的类型                             |
| 报表名称  | 此查询的名称                             |
| 所属部门  | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 查询条件  | 选择进程查询条件                           |
| 时间范围  | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| 操作系统  | 选择操作系统                             |
| IP 地址 | 输入要查询的 IP 地址                       |
| 主机名   | 输入要查询的主机名                          |

| \$25%A 131    | 12556 法内部法     |      |       |               |                     |
|---------------|----------------|------|-------|---------------|---------------------|
| TT-MAN        | 1.55           | 創口お用 | 25.08 | <b>联位:</b> 市地 | 上展目目                |
| 10.201 140.1  | admin-yangweie |      | 300   | Windows XP    | 2012/10/29 10:51:21 |
| 10,201 185.27 | WDN-ywwiii     | (m)  | 340   | Windows 7     | 2012/11/1 10:41:44  |

计算机帐号查询


| 报表类型                                | 计算机帐号查询      |          |                     |                 |                  |         |          |            |                            |                                    |
|-------------------------------------|--------------|----------|---------------------|-----------------|------------------|---------|----------|------------|----------------------------|------------------------------------|
| 报表名称                                | 计算机帐号查询      |          |                     |                 |                  |         |          |            |                            |                                    |
| 所属部门                                | 所有部门         |          |                     |                 | 2.               | 选择部门    |          |            |                            |                                    |
| IP地址范围                              |              |          |                     | -               |                  |         |          |            |                            |                                    |
| 查询组合条件                              | 10 38 2      | 19 🗆 11  | 锁定 🗏 🗄              | 码过期             | (密               | 月过期     | NRX      | winXPU)    | 上系統                        | E效)                                |
| 指定计算机名                              |              |          |                     |                 |                  |         |          |            |                            |                                    |
| 帐号可用性                               | 不指定          | ŝ.       |                     |                 |                  |         |          |            |                            |                                    |
| <u> </u>                            | 所有           |          |                     |                 |                  |         |          |            |                            | 1                                  |
| 创建状态<br>创建者                         | 全局<br>admini | strator  |                     |                 |                  |         |          |            |                            |                                    |
|                                     | 保存           | 并执行      | 保存                  |                 | 1                | hfi     |          |            | iş (                       | 取消                                 |
| 配置项:                                |              | 说        | 明                   |                 |                  |         |          |            |                            |                                    |
| 报表类型                                |              | 此        | 企面的                 | り类              | 型                |         |          |            |                            |                                    |
| 报表名称                                |              | Щ        | 查询的                 | <b></b>         | 称                |         |          |            |                            |                                    |
| 所属部门                                |              | 选<br>击   | 译需要<br>千 <b>"选择</b> | 要查<br><b>译部</b> | 询的<br><b>门"</b>  | ッ终<br>来 | 端所<br>进行 | 斤属的<br>亍选择 | り部广<br>≰                   | ],也可点                              |
| IP 地址范围                             |              | 进        | 择进利                 | 呈查              | 询条               | 件       |          |            |                            |                                    |
| 查询组合条件                              |              | 进        | 择帐号                 | 子查              | 询组               | [合      | 条作       | <b>†</b>   |                            |                                    |
| 指定计算机名                              |              | 输        | 认要查                 | 至询              | 的计               | ·算      | 机名       | 3          |                            |                                    |
| 帐号可用性                               | 选择帐号属性       |          |                     |                 |                  |         |          |            |                            |                                    |
| 帐号类型                                |              | 进        | 择帐号                 | 子类              | 型                |         |          |            |                            |                                    |
| 计算机数号直接<br>                         | 2262<br>275  | Nes-     |                     | 638             | 11 <sup>22</sup> | -       | No.      | - Enu      | 11252                      |                                    |
| 01 b45                              | men          | ASPIRET  |                     | 習慣用             | 2                |         | 2        |            | g the Al<br>rocess (<br>e) | P.NET worker p<br>appnet_wp.ex     |
| 01 b45                              | -149         | RISK_VEN | WIS-REALERS         | pi and ref      |                  |         |          |            | 第名の月<br>有的内容<br>第三〇〇       | Weathan 信息板<br>他内<br>のWaathand waa |
| 01 b43                              | men          | BALO     | W/D-KSYEB           | Navi            |                  |         | 5        |            | Inferred<br>B/P            | 1. 印刷影响自己的图                        |
| 172 25 254.1 venue 638796<br>01 b45 | 间电荷          | autorige |                     | 普通用             | 4                | *       | #.       | 4          | 道地松行                       | 中心服育性内                             |

#### 黑名单进程违规历史查询

172.25.254.) venus-638956 01 645

<u>172.75.254.1</u> venus-638950 mjš(쪽 kess181 01 b45

<u>172,25254.1</u> venus-63856 mj性用 SLEPORT\_388945a0 普通用 基 集 重 01 b45 //

ASPNET

前後用 臣 臣 臣 臣

这進一个群點和快快紛后的權 共產黨的

Account used for runnin g the ASP NET worker p rocess (aspinet\_wp.es e)





| 配置项:  | 说明                                 |  |  |  |
|-------|------------------------------------|--|--|--|
| 报表类型  | 此查询的类型                             |  |  |  |
| 报表名称  | 此查询的名称                             |  |  |  |
| 所属部门  | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |  |  |  |
| 查询条件  | 选择进程查询条件                           |  |  |  |
| 时间范围  | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |  |  |  |
| 操作系统  | 选择操作系统                             |  |  |  |
| IP 地址 | 输入要查询的 IP 地址                       |  |  |  |
| 主机名   | 输入要查询的主机名                          |  |  |  |

| 素名里這程知       | 開助安全會    |       |                   |              |               |                     |
|--------------|----------|-------|-------------------|--------------|---------------|---------------------|
| 输动程表         | 华北西东     | 是为能油  | E.                |              |               |                     |
| IP MIN       | 18.64    | #CI2A | marcheld.         | 机压机器         | 推住系统          | 2.5010              |
| 177,25,1,290 | 中交主机构    |       | 6C-62-6D-48-E2-71 | noteped eve  | Windows 7 x64 | 2012/30/25 19:36:19 |
| 172,25,1 200 | 中立主机器    |       | 6C-62-6D-46-E2-71 | nitepad.exe  | Windows 7 e64 | 2012/10/25 19:36:19 |
| 172/23 1 200 | 中交主机高    |       | 6C-62-6D-06-62-71 | notepad.exe  | Windows 7 x64 | 2012/30/23 19:36:19 |
| 172,25,1,200 | 中文家彩彩    |       | 6C-62-6D-46-82-71 | notepad ave  | Windows 7 x64 | 2612/10/25 19:36:19 |
| 172.29.1.200 | 中交出机构    |       | 6C-62-6D-48-E2-71 | nutepad.exe  | Windows 7 x64 | 2012/30/23 19:30:19 |
| 172,25,1,200 | 中文正彩岩    |       | 6C-62-6D-46-E2-71 | ave.bcqetten | Windows 7 x64 | 3013/30/25 19:39:01 |
| 172.25.1.200 | 中交击机构    |       | 6C-62-6D-48-62-71 | notepad.exe  | Windows 7 x64 | 2012/20/25 19:39:01 |
| 172.25 1.200 | 中交主机品    |       | 6C-62-6D-46-E2-71 | ava begatan  | Windows 7 x64 | 2012/30/25 19:39:01 |
| 172 25 1 200 | 中京主教員    |       | 6C-62-6D-46-E2-71 | notepiad.exe | Windows 7 x54 | 2012/10/25 19:39:01 |
| 172,25.1.200 | 中文主彩名    |       | 6C-62-6D-46-E2-71 | notepad.exe  | Windows 7 x64 | 2012/10/25 10:39:01 |
| 1012232      | 178910-3 | đ     |                   |              |               | 第1百/共共22百219年的調     |

白名单进程违规历史查询



| 报表类型 | 进程违规历史查询      |          |        |
|------|---------------|----------|--------|
| 报表名称 | 白名单进程违规历史查询   |          |        |
| 查询条件 | 白名单           |          |        |
| 所属部门 | 所有部门          |          | ▼ 选择部门 |
| 时间范围 | ● 最近 7<br>○ 从 | 天<br>回 到 |        |
| 操作系统 | 不指定           | 1.000    | *      |
| IP地址 |               |          |        |
| 主机名  |               |          |        |
| 创建状态 | 全局            |          |        |
| 创建者  | administrator |          |        |
|      |               |          |        |

| 保存并执        | 行 保存 执行 删除 取消                                 |  |  |  |  |  |
|-------------|---|--|--|--|--|--|
| 配置项:        | 说明  |  |  |  |  |  |
| 报表类型        | 此查询的类型  |  |  |  |  |  |
| 报表名称        | 此查询的名称  |  |  |  |  |  |
| 所属部门        | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择            |  |  |  |  |  |
| 查询条件        | 选择进程查询条件                                      |  |  |  |  |  |
| 时间范围        | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围              |  |  |  |  |  |
| 操作系统        | 选择操作系统  |  |  |  |  |  |
| IP 地址       | 输入要查询的 IP 地址                                  |  |  |  |  |  |
| 主机名         | 输入要查询的主机名                                     |  |  |  |  |  |
| 自名学讲校击线历史音演 | mer <u>ing 在日本市 前日本市 主新时间</u><br>重10/开有+司の存在第 |  |  |  |  |  |

强制补丁违规历史查询



| 报表类型 | 强制补丁违规历史查询    |                     |        |
|------|---------------|---------------------|--------|
| 报悉名称 | 强制补丁违规历史查询    | 1                   |        |
| 所屬創门 | 所有部门          |                     | - 选择部门 |
| 时间范围 | ● 最近 7<br>○ 从 | 夫<br>回 <sub>到</sub> |        |
| 操作系统 | 不描定           |                     |        |
| IP地址 |               |                     |        |
| 主机名  |               |                     |        |
| 创建状态 | 全期            |                     |        |
| 创建奏  | administrator |                     |        |

| 保存并执行 | ī 保存 执行 删除 取消                               |
|-------|---|
| 配置项:  | 说明  |
| 报表类型  | 此查询的类型                                      |
| 报表名称  | 此查询的名称                                      |
| 所属部门  | 选择需要查询的终端所属的部门,也可点<br>击 <b>"选择部门"</b> 来进行选择 |
| 时间范围  | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围            |
| 操作系统  | 选择操作系统                                      |
| IP 地址 | 输入要查询的 IP 地址                                |
| 主机名   | 输入要查询的主机名                                   |

| 西利普丁法·累历<br>628 年8 53 | 生產用<br>2.約8 (1.5.1018) |        |           |           |                     |
|-----------------------|------------------------|--------|-----------|-----------|---------------------|
| 11184                 | 15.68                  | 181184 | BIAR      | 85.5%     | 2.001/0             |
| 10.201 140 27         | with-yangweie          |        | KB2731847 | Windows 7 | 2012/10/30 15:43:26 |
| 10 201 140 27         | WIN-yangweie           | -09    | HB2733847 | Windows 7 | 2012/10/30 15:44:23 |
| 20,201,140,27         | Wills-years            | mi     | K82731847 | Windows 7 | 2012/11/1 0:47:34   |
| 1                     |                        |        |           |           | 第1页/共有1页3年数据        |

病毒码违规历史查询





| TR 11 VE DC | 11 18-11 19-11 19-11 19-11         |  |  |  |  |  |
|-------------|------------------------------------|--|--|--|--|--|
| 配置项:        | 说明                                 |  |  |  |  |  |
| 报表类型        | 此查询的类型                             |  |  |  |  |  |
| 报表名称        | 此查询的名称                             |  |  |  |  |  |
| 所属部门        | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |  |  |  |  |  |
| 时间范围        | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |  |  |  |  |  |
| 操作系统        | 选择操作系统                             |  |  |  |  |  |
| IP 地址       | 输入要查询的 IP 地址                       |  |  |  |  |  |
| 主机名         | 输入要查询的主机名                          |  |  |  |  |  |
| 病毒码违规历史查查   |                                    |  |  |  |  |  |

| IPHN -        | 上风起来          | 0136.0 | 酸色系统      | 68/78    | TERME               |
|---------------|---------------|--------|-----------|----------|---------------------|
| 10.293 100.77 | jingjun-X64xp | 719    |           | 防伤毒未充其   | 2012/30/29 17:32:46 |
| 10.201.140.27 | WIN-yangweie  |        | Windows 7 | 防由草木定县   | 2012/10/38 15:34:04 |
| 10.201.140.27 | WIN-yangweie  | -0     | Windows 7 | 防肉毒未安菜   | 2012/10/30 15:44:24 |
| 10,201.140,27 | WIN-yangwee   | -8     | Windows 7 | 动物导生生的   | 2012/30/30 15:44:25 |
| 10.201.140.27 | WIN-yangweie  | -0     | Windows 7 | 的内容不会说   | 2012/30/30 15:46:26 |
| 10.291.140.27 | WIN-yangweie  |        | Windows 7 | 而由草木田岡   | 2012/30/30 15:47:00 |
| 10/201140.21  | W04-yangweie  | -0     | Windows 7 | 0.0619.2 | 2012/30/36 13 48 30 |
| 10.201.140.27 | WIN-yangwee   | -9     | Windows 7 | 印纳莱卡尔派   | 2012/30/38 15:49:00 |
| 10.201.140.27 | WIN-yangweie  | -0     | Windows 7 | 历代春末安装   | 2012/10/30 15:51:01 |
| 10.201 140.27 | WIN-yangweie  | -8     | Windows 7 | 市由基本定例   | 2012/10/38 15:56:32 |
| 1123520EE     |               |        |           |          | #15/##45532##       |

安全加固-域策略违规历史查询



| 报表类型   | 安全加固-域策略违规历史查询      |                                    |      |        |        |  |  |
|--|---------------------|------------------------------------|------|--------|--------|--|--|
| 报表名称   | 安全加固-域策略违规历史查询      |                                    |      |        |        |  |  |
| 所属部门   | 所有部门                |                                    |      |        | ▼ 选择部门 |  |  |
| 时间范围   | ◎ 最近 7              |                                    | F    |        |        |  |  |
|  | © M                 |                                    | 1 到  |        |        |  |  |
| 操作系统   | 不指定                 |                                    |      |        | *      |  |  |
| IP地址   |                     |                                    |      |        |        |  |  |
| 主机名  |                     |                                    |      |        |        |  |  |
| 创建状态   | 全局                  |                                    |      |        |        |  |  |
| 创建者  | administrato        | or                                 |      |        |        |  |  |
|  | 保存并执行               | 保存                                 | 执行   | 删除     | 取消     |  |  |
| 配置项:   |                     | 说明                                 |      |        |        |  |  |
| 报表类型   |                     | 此查询的类型                             |      |        |        |  |  |
| 报表名称   |                     | 此查询的名称                             |      |        |        |  |  |
| 所属部门   |                     | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |      |        |        |  |  |
| 时间范围   |                     | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |      |        |        |  |  |
| <b>操作系统</b> 选择操作系统                             |                     |                                    |      |        |        |  |  |
| IP 地址  | 输入要查询的 IP 地址        |                                    |      |        |        |  |  |
| 主机名  | <b>l名</b> 输入要查询的主机名 |                                    |      |        |        |  |  |
| 安全加四-回茶味出現<br>取みまま - 日本市<br>10000 - 111月日<br>1 | 防史意識<br>(           | ANA BERM                           | 8.00 | 80.514 |        |  |  |

白名单软件安装违规历史查询





| 配置项:  | 说明                                 |
|-------|------------------------------------|
|       |                                    |
| 报表类型  | 此查询的类型                             |
| 报表名称  | 此查询的名称                             |
| 查询条件  | 选择进程查询条件                           |
| 所属部门  | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围  | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| 操作系统  | 选择操作系统                             |
| IP 地址 | 输入要查询的 IP 地址                       |
| 主机名   | 输入要查询的主机名                          |

| 1710.04       | 10.00         | Increase. | 8048            | 60.5%     | 2.80101             |
|---------------|---------------|-----------|-----------------|-----------|---------------------|
| 0.201.140.27  | WIN-yangereis |           | 360#2P±         | Windows 7 | 2012/10/26 12:02:43 |
| 0.201 140.27  | WIN-yangweie  | 一切        | QQProtect       | Windows 7 | 2012/10/26 12:02:42 |
| 10 201 140 27 | WIN-yangesie  |           | QQ软件繁臻1.0 Beta3 | Windows 7 | 2012/10/26 12:02:43 |
| 10 201 140 27 | WIN-yangweie  | 一切        | 費(LQQ2012(安全的把) | Windows 7 | 2012/10/26 12:02:42 |
| 10 201 140 27 | WIN-yangeute  | 0         | 360世立卫士         | Windows 7 | 2013/10/26 13:57:45 |
| 10 201 140 27 | WIN-yangweie  | -49       | QQProtect       | Windows 7 | 2012/10/20 13:57:45 |
| 10,201,140,27 | WIN-yangwale  |           | QQ的仲教證1.0 Beta3 | Windows 7 | 2012/10/26 13:57:45 |
| 10 201 140 27 | WIN-yangweie  | —in       | 費法QQ2012(安全的約)  | Windows 7 | 2012/10/26 13:57:45 |
| 10.201.140.27 | WIN-yangwere  | —册        | 360#221         | Windows 7 | 2012/10/26 13:58:49 |
| 10,201,140,27 | WIN-yangweie  | 一切        | QQProtect       | Windows 7 | 2012/10/20 13:58:45 |

红名单软件安装违规历史查询





| 配置项:  | 说明                                 |
|-------|------------------------------------|
| 报表类型  | 此查询的类型                             |
| 报表名称  | 此查询的名称                             |
| 查询条件  | 选择进程查询条件                           |
| 所属部门  | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围  | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| 操作系统  | 选择操作系统                             |
| IP 地址 | 输入要查询的 IP 地址                       |
| 主机名   | 输入要查询的主机名                          |

| 安全基线查谢与                 | 接计                             |        |      |        |        |              |
|-------------------------|--------------------------------|--------|------|--------|--------|--------------|
| <u>红名单软件</u><br>编改统计 耳( | 安装 <u>击版历史者</u><br>[四本] [录为前法] | h      |      |        |        |              |
| 1.1.64                  | macifist                       | 109201 | 教教会部 | 60.848 | LUEBUI | <b>208</b>   |
| 1                       |                                |        |      |        |        | 第1页/共有1页0条数据 |

黑名单软件安装违规历史查询





| 配置项:  | 说明                                 |
|-------|------------------------------------|
| 报表类型  | 此查询的类型                             |
| 报表名称  | 此查询的名称                             |
| 查询条件  | 选择进程查询条件                           |
| 所属部门  | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围  | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| 操作系统  | 选择操作系统                             |
| IP 地址 | 输入要查询的 IP 地址                       |
| 主机名   | 输入要查询的主机名                          |

#### 红名单软件安装违规历史重调 45.888 0.9888 0.9884

| III III III   | 1.8.8.8         | 10161 | Read Read | 版() 系统         | LIMIS               |
|---------------|-----------------|-------|-----------|----------------|---------------------|
| 10.201.115.8  | 32648638        |       | state     | Windows XP x64 | 2012/50/25 15:48:13 |
| 10.201 140 27 | W3N-yangweie    | ip    | 84        | Winduwa 7      | 2012/10/26 9:52:43  |
| 10.201.148.27 | WINi yangwele   | 92    | 88.       | Windows 7      | 2012/10/26 9:53:43  |
| 10.201.140.27 | WIN-yangwele    | -07   | 7.00      | Windows 7      | 2812/30/28 10:04:04 |
| 10.201.140.27 | WIN-yangwele    | -92   | 展示        | Windows 7      | 2012/10/26 10:04:05 |
| 10.201 140 27 | WIN-yangweie    | -179  | 360       | Windows 7      | 2012/30/26 10:17:05 |
| 10.201 148 27 | With yangwele   |       | 360       | Windows 7      | 3012/10/26 10:17:05 |
| 10.201.23.27  | W1N-QUBBERK11EQ | -10   | 300       | Windows 7      | 2012/30/20 10:37:43 |
| 10.201 23.117 | WIN-NEUOTOSSEM  | -92   | 360       | Windows 7 x64  | 2012/10/26 10:17:55 |
| 10.201 72.2   | venus-518c94044 | -49   | 366       | Windows XP     | 2012/10/26 10:16:05 |
| 1234387       | 8 8 10 - MD     |       |           |                | 第1页/共有20页100条数据     |

红名单软件安装违规状态查询





| 保存并执行                           | <b>「」 保存 払行 删除 取消</b>              |  |  |  |  |  |
|---------------------------------|------------------------------------|--|--|--|--|--|
| 配置项:                            | 说明                                 |  |  |  |  |  |
| 报表类型                            | 此查询的类型                             |  |  |  |  |  |
| 报表名称                            | 此查询的名称                             |  |  |  |  |  |
| 查询条件                            | 选择进程查询条件                           |  |  |  |  |  |
| 所属部门                            | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |  |  |  |  |  |
| 时间范围                            | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |  |  |  |  |  |
| 操作系统                            | 选择操作系统                             |  |  |  |  |  |
| IP 地址                           | 输入要查询的 IP 地址                       |  |  |  |  |  |
| 主机名                             | 输入要查询的主机名                          |  |  |  |  |  |
| 红名单数件安装法院获高资务<br>资源服务 驾洽服务 通为商商 |                                    |  |  |  |  |  |

| TIMEN         | 13.0           | 1000 | 軟件品則 | 输生系统         | 上版以目                |
|---------------|----------------|------|------|--------------|---------------------|
| 172,25,29,123 | cat)           | -0   | 99   | Windows 2003 | 2012/10/01 15:28:58 |
| 10 201,140.1  | admin-yangkese | -40  | alsc | Windows XP   | 3013/30/39 10:51:31 |
| 10.201 140.22 | WDV-pwe        | mj   | abc  | Windows 7    | 2012/13/1 10:41:44  |
| 1             |                |      |      |              | 第1四/共有1万3条数据        |

终端共享资源查询



| 报表类型   | 终端共享资源查询  |   |          |
|--------|---|---|----------|
| 报表名称   | 终端共享资源查询  |   |          |
| 所属部门   | 所有部门  | • | 选择部门     |
| IP地址范围 |   |   |          |
| 共享资源类型 | 不指定   | - |          |
| 创建状态   | 全局  |   |          |
| 创建者    | administrator   |   |          |
|        | /0 左 并 执 在 10 左 14 左 11 10 10 10 10 10 10 10 10 10 10 10 10 |   | Win 2015 |
|        |   | 6 | 取用       |

| 配置项:   | 说明                                       |
|--------|--|
| 报表类型   | 此查询的类型                                   |
| 报表名称   | 此查询的名称                                   |
| 所属部门   | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择       |
| 时间范围   | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围         |
| 共享资源类型 | 可以"不指定"类型,或选择文件共享,打印机<br>共享, IPC\$共享进行查询 |

| 和政策推进              | -11100 M 3K.498 St                     |      |                       |                     |                      |                         |
|--------------------|--|------|-----------------------|---------------------|----------------------|-------------------------|
| IPRM.              | IRA                                    | 2006 | 100.1212              | 共安直導                | REAM                 | LAND                    |
| 10,701,100,2<br>10 | win2008x84testworkse<br>rver202222222  | -0   | 6C-62-60-07-6<br>1-M  | 又件共舉F:103           | Windows 2008 x<br>64 | 2012/10/01 17:0<br>6:43 |
| 10.201.100.2<br>05 | win200Ex64testworkse<br>rver2022222222 | -@   | 6C-62-60-07-6<br>1-AF | 文件共要C:\Windo<br>Wii | Windows 2008 s<br>64 | 2012/10/31 17:0<br>6:43 |
| 10,701,100,2<br>09 | win2008x84testworkse<br>rver202222222  | -01  | 6C-62-60-07-6<br>1-MF | 文件共業に当              | Windows 2008 x<br>64 | 2012/10/31 17:0<br>5:43 |
| 10.201.100.2       | win200Ex64testworkpe<br>rver2022222222 | -91  | 8C-62-60-07-6<br>1-AF | 文件共要并在              | Windows 2008 s<br>64 | 2012/10/31 17:0<br>6:43 |
| 19,291,109,2       | win200Ex84testworkse<br>tver2022222222 | -0   | 8C-82-6D-07-6<br>1-M  | 文明和歌作行              | Windows 2008 x<br>64 | 2012/18/31 17:0<br>6:43 |
| 10.201.100.2       | wm2008x64bastworkpe<br>rver2022222222  | -91  | 6C-62-60-07-6<br>1-AF | 文件书章6八              | Wesdows 2008 x<br>64 | 2012/10/31 17:0<br>6:43 |
| 10/201 100/2       | win2008x64testworkse<br>rver2022222222 | -19  | 8C-62-60-07-6<br>1-AF | 交件非单6:\             | Windows 2008 x 64    | 2012/10/31 17:0<br>6:43 |
| 10,201,100,2<br>26 | win2008x54testworkse<br>rver2022222222 | -8   | 6C-62-6D-D7-6<br>1-AF | <b>文件共華H:</b> \     | Windows 2008 x<br>54 | 2012/10/34 17:0<br>5:43 |
| 10.261.100.2<br>25 | win2008X64testworkse<br>rver202222222  | -19  | 6C-62-60-07-6<br>1-AF | 文件共审F:VOS DV<br>D   | Wexdows 2008 x<br>04 | 2012/18/31 17:0<br>0:43 |
| 10.201.100.2       | win2008x64testworkse<br>rver2022222222 | -91  | 6C-62-6D-07-6<br>1-AF | 文件共审F:/soft         | Windows 2008 x 64    | 2012/10/31 17:0<br>6:43 |

| 启明星辰                        |
|-----------------------------|
| http://www.venustech.com.cn |



## 15.7. 外联控制

## 15.7.1. 配置介绍

外联控制记录了外设违规,多网卡,异常路由。

请选择查询统计图表类型:

| 、王大、 | © 终端非法外联违规TopN    |  |  |  |  |  |  |
|------|-------------------|--|--|--|--|--|--|
|      | ◎ 非法外联不合规网段统计TopN |  |  |  |  |  |  |
|      | ◎ 曾经发生多网卡外联行为终端统计 |  |  |  |  |  |  |
|      | ◎ 客户端多网卡外联历史查询    |  |  |  |  |  |  |
|      | ◎ 客户端多网卡外联快照查询    |  |  |  |  |  |  |
|      | ◎ 终端多网卡违规查询       |  |  |  |  |  |  |
|      | ◎ 外设违规查询          |  |  |  |  |  |  |
|      | ◎ 异常路由查询          |  |  |  |  |  |  |
|      | ◎ USB设备使用历史查询     |  |  |  |  |  |  |
|      | ◎ 非法外联告警查询        |  |  |  |  |  |  |
|      | ◎ 终端违规拨号查询        |  |  |  |  |  |  |
|      | 下一步 取消            |  |  |  |  |  |  |
|      |                   |  |  |  |  |  |  |

#### 外设违规查询

| 报表类型 | 外资速度查询             |  |  |  |  |  |
|------|--------------------|--|--|--|--|--|
| 报表名称 | 外疫性機管理             |  |  |  |  |  |
| 所属部门 | 所有部门 - 选择部门        |  |  |  |  |  |
| 操作系统 | 不指定・               |  |  |  |  |  |
| IP地址 |                    |  |  |  |  |  |
| 主机名  |                    |  |  |  |  |  |
| 创建状态 | 全局                 |  |  |  |  |  |
| 创建有  | administrator      |  |  |  |  |  |
|      | 保存并执行 保存 执行 删除 取消  |  |  |  |  |  |
| 配置项: | 说明                 |  |  |  |  |  |
| 查询类型 | <b>美型</b> 此查询的类型   |  |  |  |  |  |
| 查询名称 | 此查询的名称             |  |  |  |  |  |
| 所属部门 | 选择需要查询的终端所属的部门,也可点 |  |  |  |  |  |
|      | 击 "选择部门" 来进行选择     |  |  |  |  |  |



| <b>操作系统</b> 选择操作系统类型 |                 |  |
|----------------------|-----------------|--|
| IP 地址                | 输入需要查询的终端 IP 地址 |  |
| 主机名                  | 输入需要查询的终端主机名    |  |

点击执行

| TITLE M.     | 1.5.1.1          | 10.010 | REAL                    | 建築売算   | <b>出水</b> 北約 | Lanci               |
|--------------|------------------|--------|-------------------------|--------|--------------|---------------------|
| 10.201.33.2  | venus-518c94044  |        | Wandows XP              | CERON  | 4            | 2012/10/30 13:30:40 |
| 10 201 33 2  | senue-518c94044  |        | Windows 30 <sup>a</sup> | CDROM  | 2            | 2012/10/30 15:44:46 |
| 10.201.33.2  | yenus-510c94044  |        | Windows XP              | CERCH  | 2            | 2012/10/30 15:45:07 |
| 10 201 33 2  | venus-518c94044  |        | Windows XP              | CDROH  | 4            | 2012/16/30 15:52:45 |
| 10,201 33 27 | WIN-QUBBEBK1JEQ  |        | Windows 7               | CORON  | I            | 2012/18/26 13:05:59 |
| 10.201.33.27 | WIN-QUBBERKITED  | miera  | Windows 7               | CEROM  | 2            | 2012/10/26 15:36:26 |
| 0.201.33.27  | WIN-QURBERKITED  | nie H  | Wandows 7               | CDROM  | 1            | 2012/10/28 20:16:03 |
| 10,203.33.27 | WIRA-CORRENKTIEC | 1040   | Windows.7               | CERCH  | 1            | 2012/10/2# 21:22:57 |
| 10,221,33,22 | WIN-QUIRBERKIEQ  | NURR   | Windows 7               | CEROH  | 1            | 2012/10/28 22:09:24 |
| 10.201.33.77 | WIN-QURRENKITEQ  | 1944   | Windows 7               | CERCIN | 1            | 2012/10/28 22:36:10 |

点击 IP 地址连接,可以查看该客户端详细报表。

#### 异常路由查询

| 探表类型     | 异常路由宣调        |    |    |     |      |
|----------|---------------|----|----|-----|------|
| 探表名称     | 异常路由查询        |    |    |     |      |
| 所實部门     | 所有部门          |    |    |     | 选择部门 |
| 皆由信息查询类型 | 查调所有路由信息      | l) |    |     |      |
| 的建状态     | 全局            |    |    |     |      |
| 创建有      | administrator |    |    |     |      |
|          | 保存并执行         | 保存 | 执行 | #R2 | 取消   |

| 配置项:   | 说明  |
|--|---|
| 查询类型   | 此查询的类型  |
| 查询名称   | 此查询的名称  |
| 所属部门   | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择  |
| 路由信息查询类型   | 选择查询的路由信息类型   |
| LANDA GURA DANA<br>ILANA LANA //Est<br>Martin LENGVO-VYGHJAT | 1 12.112 Interime 87.8.0 65.8.0<br>172.25.0.1 172.25.85.254 2012-10-30 17:41:24 2012-10-30 17:41:24 |

第1页/用用1页1条数据

| 终端名 | 网卡讳规杳询 |  |
|-----|--------|--|

1





| 配置项:                        | 说明                                 |  |  |  |  |
|-----------------------------|------------------------------------|--|--|--|--|
| 查询类型                        | 此查询的类型                             |  |  |  |  |
| 查询名称                        | 此查询的名称                             |  |  |  |  |
| 所属部门                        | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |  |  |  |  |
| 操作系统                        | 选择操作系统类型                           |  |  |  |  |
| IP 地址                       | 输入需要查询的终端 IP 地址                    |  |  |  |  |
| 主机名                         | 输入需要查询的终端主机名                       |  |  |  |  |
| 时间范围                        | 选择时间范围                             |  |  |  |  |
| In his or one hand an entry |                                    |  |  |  |  |

| 8.0.WA 5       | 法拥有 放为机法     |       |         |         |       |                     |
|----------------|--------------|-------|---------|---------|-------|---------------------|
| 174036         | 1.0.60       | 10115 | 165.518 | 1.00.00 | 38X0  | Lance               |
| 192.166.88.112 | Kusk-notepad |       |         |         | - L.: | 2012/10/27 14:13:33 |
| 1              |              |       |         |         |       | #15(3817)200        |

#### 客户端多网卡外联快照查询





第1页/州内1页1条数据

2012/10/27 14:13:3

第1页/共有1页1页数建

2

| 查询名称 |                  | 此了   | 此查询的名称             |                    |                |  |    |
|------|------------------|------|--------------------|--------------------|----------------|--|----|
| 所属部门 |                  | 选择击  | 释需要<br>" <b>选择</b> | 查询的约<br><b>部门"</b> | &端所属的<br>そ进行选择 | <b>部门,也</b>                              | 可点 |
|      | X 休田 小 府<br>(明本) | MORN | MACRIE             | ARRIE              | damardan<br>B  | ANKA                                     |    |
| 1    |                  |      |                    |                    |                | an a |    |

## 客户端多网卡外联历史查询

#### 客户城多同卡外联历史查询 报表类型 报责名称 客户诸多同卡外联历史查询 所属部门 ▼ 选择部门 新有部门 主机名 时间范围 ■截近7 <u>म</u> 1 OA IP地址范围 创建状态 全局 创建有 administrator 保存并执行 保存 执行 取消 1003

| 配置项:    | 说明                                 |
|---------|------------------------------------|
| 査询类型    | 此查询的类型                             |
| 查询名称    | 此查询的名称                             |
| 所属部门    | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| IP 地址范围 | 输入需要查询的终端 IP 地址范围                  |
| 主机名     | 输入需要查询的终端主机名                       |
| 时间范围    | 选择时间范围                             |
|         | n gant sana gan ann agusann na     |

曾经发生多网卡外联行为终端统计

102 106 10 11 Kuck-notepa



| 报表类型                         | 曾经发生多网卡外国     | 行力均满块  | H         |     |        |
|------------------------------|---------------|--------|-----------|-----|--------|
| 振表氣務                         | 曾经发生多月卡州      | 联行为终端统 | ił        |     |        |
| 新麗部门                         | 所有部门          |        |           |     | - 法释部门 |
| 时间范围                         | ● 最近 7<br>○ A |        | 天<br>田 19 |     |        |
| 是否排除闷卡数为2<br>且有WLAN问卡的<br>电脑 | *2.05         |        |           |     |        |
| 创建状态                         | 全局            |        |           |     |        |
| 0( <b>2</b> 4                | administrator |        |           |     |        |
|                              | 保存并执行         | 保存     | 执行        | MER | 取消     |

| 配置项:                            | 说明                                 |
|---------------------------------|------------------------------------|
| 查询类型                            | 此查询的类型                             |
| 查询名称                            | 此查询的名称                             |
| 所属部门                            | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围                            | 选择时间范围                             |
| 是否排除网卡数为 2<br>且有 WLAN 网卡的电<br>脑 | 选择是否排除掉有两块网卡,且有无线网<br>卡的电脑         |

| 首经发生多同于<br>单次起表 55 | 外联行为终端:<br>出開表 - 最为 | <del>法计</del><br>mit |           |       |                     |          |
|--------------------|---------------------|----------------------|-----------|-------|---------------------|----------|
| 10 Million         | 15.04               | DECEMBER MANAGEME    | #26AA0911 | 388.6 | AMLINICA            | america  |
| 192.108.00.112     | Kuck-notepied       |                      | 13        |       | 2912/30/27 14:33:33 |          |
| 1                  |                     |                      |           |       | 第100                | 共和1页1条数语 |

#### 非法外联不合规网段统计 Top10





| 配置项: | 说明                                 |
|------|------------------------------------|
| 查询类型 | 此查询的类型                             |
| 查询名称 | 此查询的名称                             |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围 | 选择时间范围                             |
| TOPN | 输入要统计的终端最大数量                       |
| 图表类型 | 选择图表类型,可选择"饼状图"和"横<br>向柱状图"        |

| WALL .         | 所在非常 | SHEAK | <b>非正则在由此以为</b> 图 |
|----------------|------|-------|-------------------|
| 10.201.33.2    | 0    | 0     | 69                |
| 10.201.33.27   | 0    | 8     | 24                |
| 192.168.88.112 | 0    | 0     | 1                 |

#### 终端非法外联违规 Top10



时间范围

图表类型

10:201-33-27

10 201 33 2

10/201 33 117

10,201 33 21

10 201 33 117

10.201.02.2

177.25.1.110

10.201.33.117

172.75.1.110

1

10.201.33.2

TOPN



终端非法外联违规Tup10 股改服条 与四面条 毫元的流

| 报表类型   | 非法外联告警查询                   |    |          |    |        |
|--------|----------------------------|----|----------|----|--------|
| 报表名称   | 非法外联告警查询                   |    |          |    |        |
| 所属部门   | 所有部门                       |    |          |    | ▼ 选择部门 |
| 时间范围   | ◎ 最近 <mark>7</mark><br>◎ 从 |    | 天<br>回 到 |    |        |
| IP地址范围 |                            |    | 4        |    |        |
| 创建状态   | 全局                         |    |          |    |        |
| 创建者    | administrator              |    |          |    |        |
|        | 保存并执行                      | 保存 | 执行       | 删除 | 取消     |

击"选择部门"来进行选择

输入要统计的终端最大数量

选择图表类型,可选择"饼状图"和"横

明前用

时间用

-8

一袋

向电开

进口枝

\*\*\*\*\*

#40817

\*#80

134

178

101

22

12

50

22

13

32

第1页/共有1页10年数据

ŝ

选择时间范围

向柱状图"

WIN-QUILERKIEQ

venue-518c94044

WIN-NSIJJTD99EM

WIN-QUBBERKIJEQ

WIN-NS20TDS9EM

venus-518:94044

renau-518c94044

WIN-NEUTOSIEM

\$1.8K-PC

KLEN-PC

| 配置项:    | 说明                                 |
|---------|------------------------------------|
| 查询类型    | 此查询的类型                             |
| 查询名称    | 此查询的名称                             |
| 所属部门    | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围    | 选择时间范围                             |
| IP 地址范围 | 选择查询的 IP 地址范围                      |

USB 设备使用历史查询





| 报表类型                         | USB设备使用                                   | US8设备使用历史查询              |                                      |  |                       |
|------------------------------|---|--------------------------|--------------------------------------|--|-----------------------|
| 报表名称                         | USB设备使                                    | 用历史查询                    |                                      |  |                       |
| 所實部门所有部门                     |   |                          |                                      | - [                                      | 法择部门                  |
| IP地址范围                       | 0   |                          |                                      |  | с. С.                 |
| 的建状态 全局<br>的建备 administrator |   |                          |                                      |  |                       |
|                              | 保存并执                                      | fī (Rf                   | ¥ 执行                                 |  | 取消                    |
| 配置工                          | 页 <b>:</b>                                | 说明                       |                                      |  |                       |
| 报表类                          | き型  | 此查询                      | 的类型                                  |  |                       |
| 报表名                          | 名称  | 此查询                      | 的名称                                  |  |                       |
| 所属音                          | 817                                       | 选择需望<br>击 <b>"选</b>      | 要查询的终端<br><b>怿部门"</b> 来进             | 所属的部门,<br>行选择                            | 也可点                   |
| IP 地址                        | 止范围                                       | 选择查试                     | 洵的 IP 地址刻                            | 古围                                       |                       |
| USB 设备使                      | <u>用历史者資</u>                              | 1                        |                                      |  |                       |
| 1228.M                       | 15.68 20                                  | 9928                     | Rif.                                 | 1000                                     | 0.2.8.0003            |
| 10.201.10                    | wir2008x5.0edworkse -0                    | Port_20001.H             | HP v230p USB Device                  | USEWED 03F08PID_SF                       | 2012/18/31<br>8:09:17 |
| 10.201.10                    | win2008X54teatworkse -®<br>rver2022222222 | Port_#0004.H<br>ub_#0003 | USB Mass Storage Devi<br>ce          | USBWID_03F06P1D_5F<br>07/6E308328728084  | 2012/16/31<br>8:06:17 |
| 10.201.10                    | wm2006x64testworkse -@<br>rver2022222222  | Pon_#0001.H<br>ub_#0004  | USB Human Interface 0<br>evice       | USEWID_04836PID_31<br>00%64.1281b0a48061 | 2012/16/31<br>8:06:17 |
| 10,201,10                    | win2005x64testworkse -®                   | Purt_+0002.H<br>ub_+0004 | USB Human Interface D<br>avice       | USBWID_04838PID_31<br>0016812d1b0a48082  | 2012/10/31<br>8:06:17 |
| 10,201,12                    | win200EX64testworkse -@                   | Port_#0002.H             | SONY DVD RW DRU-V20<br>OA USB Device | USEWID_0484APID_68<br>30/087100011848841 | 2012/10/31<br>8:09:37 |
| 10,201,19                    | win2008x64testworkse -@                   | Port_+0004.H             | Generic Rash Disk USB<br>Device      | USBWID_058F8PID_63<br>87(9981A011        | 2012/18/31<br>8:06:17 |

10.201.10 wm2008X64testworkse =# Purt\_E0001.H SAMSUNG G1 Portable USEVUD\_058F6PID\_63 2012/10/31 12200 rver20222222222 USE USE Portable USE Device Statistic Control (Control (Control

# 15.8. 攻击告警

## 15.8.1. 配置介绍

| <u>攻击告警查询与统计</u> |                |
|------------------|----------------|
| 请选择查询统计图表类型:     | ◎ 告警次数历史统计     |
|                  | ◎ 统计告警事件最多TopN |
|                  | ◎ 告警事件查询       |
|                  | ARP欺骗次数统计      |
|                  | ◎ 客户端防火墙日志查询   |
|                  | 下一步 取消         |

#### 告警事件查询

通过对指定的告警事件类型,日期,IP 等的组合查询特定的告警 事件。





| 主机名     | 输入要查询的终端主机名                      |
|---------|----------------------------------|
| 时间范围    | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围 |
| IP 地址范围 | 输入要查询的终端 IP 地址范围                 |
| 告警类型    | 选择告警类型                           |
| 告警子类型   | 选择告警子类型                          |

<u>地名古德波利与拉计</u>

| <u>告賢事</u><br>「総政策社 | 1 <u>点的</u><br>[15:2008_ 毫为的 | a     |      |      |              |
|---------------------|------------------------------|-------|------|------|--------------|
| BIAE                | IT M M                       | BELSE | 2552 | 2825 | 0.5:10       |
| 1                   |                              |       |      |      | 第1五/共有1页0条数8 |

#### 客户端防火墙日志查询

| 报表类型 | 客户端防火墙日志亚谓    |    |                     |      |      |
|------|---------------|----|---------------------|------|------|
| 报表名称 | 客户编历火通日志宣调    | l. |                     |      |      |
| 新聞部门 | 所有部门          |    |                     |      | 选择部门 |
| 时间想到 | ● 最近 7<br>○ 从 |    | <del>х</del><br>Ш э |      |      |
| 即地址  |               |    |                     |      |      |
| 端口   |               |    |                     |      |      |
| 方向   | 所有            |    |                     |      |      |
| 集顿   | 所有            |    |                     |      |      |
| 制作   | 所有            |    |                     |      | 5    |
| 创建状态 | 全間            |    |                     |      |      |
| 创建奏  | administrator |    |                     |      |      |
|      | 保存并执行         | 保存 | 执行                  | BHER | 取消   |

| 配置项:  | 说明                                 |
|-------|------------------------------------|
| 报表类型  | 此报表的类型                             |
| 报表名称  | 此报表的名称                             |
| 所属部门  | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围  | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| IP 地址 | 输入要查询的终端 IP 地址                     |



| 端口 | 输入要查询的日志中匹配的端口号 |
|----|-----------------|
| 方向 | 选择连入或连出         |
| 协议 | 选择协议            |
| 动作 | 选择防火墙的动作类型      |

| 行口编制的   | 《着日志查    | <u>A</u> |          |      |                   |      |      |
|---------|----------|----------|----------|------|-------------------|------|------|
| etxist. | CANA DES | SEL .    | 10000000 | <br> | <br>CONTRACTOR OF | <br> | <br> |

### ARP 欺骗次数统计

| 现古古香宣词与说刘 |                   |    |
|-----------|-------------------|----|
| 报表类型      | ARP就编文教统计         |    |
| 报表名称      | ARP欺骗大批统计         |    |
| 所属卸门      | 所有部门 ★ 送理部        | N] |
| 时间范围      | ● 最近 7 天          | _  |
|           | O A B B B         |    |
| 图表类型      | 0 无图              |    |
|           | ◎ 詳述図             |    |
|           | ● 横向柱状图           |    |
| 创建状态      | 全局                |    |
| 创建者       | administrator     |    |
|           | 保存并执行 保存 执行 删除 取消 | i  |

| 配置项: | 说明                                 |
|------|------------------------------------|
| 报表类型 | 此报表的类型                             |
| 报表名称 | 此报表的名称                             |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围 | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |



| 我也自愿着我与我计           ASP 欺骗:次放抗计           能动情计:         四出版集           我的:         四出版集 | 图表类型                                       | 选择图录<br>向柱状图 | 長类型,可选择 <b>"</b> 6<br><b>图"</b> | 并状图"和"横 |
|---|--|--------------|---------------------------------|---------|
|   | 未由自要资料与统计<br>ASPI防盗法会数统计<br>能动标识 国际组织 得为消退 | #718.8       |                                 |         |

#### 统计告警事件最多 Top10

| 报表类型 | 统计告警事件最多Top/  | 1   |     |      |
|------|---------------|-----|-----|------|
| 报表名称 | 统计告警事件最多Top   | 10  |     |      |
| 新属部门 | 所有部门          |     | - 📑 | き探部门 |
| 时间范围 | @ 最近 7        | Ŧ   |     |      |
|      | O M           | E y | =   |      |
| TopN | 10            |     |     |      |
| 图表类型 | ◎ 元图          |     |     |      |
|      | 0 讲状图         |     |     |      |
|      | ◎ 横向柱状图       |     |     |      |
| 创建状态 | 全局            |     |     |      |
| 创建者  | administrator |     |     |      |

| 配置项: | 说明                                 |
|------|------------------------------------|
| 报表类型 | 此报表的类型                             |
| 报表名称 | 此报表的名称                             |
| 所属部门 | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围 | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| TOPN | 输入要统计的终端最大数                        |
| 图表类型 | 选择图表类型,可选择"饼状图"和"横<br>向柱状图"        |



| 设计告数事件最多T                  | 010  |      |  |
|----------------------------|------|------|--|
| Table is a substant in the | 2022 | 5522 |  |
|                            |      |      |  |

#### 告警次数历史统计

| 报表类型         | 告警次数历史统计            |       |
|--------------|---------------------|-------|
| 报表名称         | 击響次數历史统计            |       |
| 所願知门         | 新有部门                | ▼ 选择部 |
| 时间地图         | ●最近7 天              | -     |
| 图表类型         | ● # L⊐ 91<br>● 7.05 | 65    |
| 0091425      | · ○ 葡萄折线图           |       |
| of建合<br>of建合 | administrator       |       |

| 配置项:  | 说明                                 |
|---|------------------------------------|
| 报表类型  | 此报表的类型                             |
| 报表名称  | 此报表的名称                             |
| 所属部门  | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围  | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| 图表类型  | 选择图表类型,可选择"饼状图"和"横<br>向柱状图"        |
| 本点無影響為な技计     古聖政教防史統計     昭和第十 国和南本 国本商法     正 |                                    |



## 15.9. 移动存储

## 15.9.1. 配置介绍

客户端使用移动存储设备时记录的审计信息



#### 移动存储管理审计

客户端使用移动存储设备时记录的审计信息

| 报表类型    | 移动存储设备        | 南计                                 |  |  |  |  |
|---------|---------------|------------------------------------|--|--|--|--|
| 报表名称    | 移动存储设备        | <b>操审计</b>                         |  |  |  |  |
| 所屬部门    | 所有部门          | • 选择部门                             |  |  |  |  |
| 时间沿面    | ● 最近 7<br>○ 从 |                                    |  |  |  |  |
| IP地址范围  |               | - II.                              |  |  |  |  |
| 操作类型    | 不描定           | •                                  |  |  |  |  |
| 创建状态    | 全局            |                                    |  |  |  |  |
| 创建者     | administrat   | tor .                              |  |  |  |  |
|         | 保存并执行         | 行 保存 しい行 明線 取済                     |  |  |  |  |
| 配置项:    |               | 说明                                 |  |  |  |  |
| 查询类型    |               | 此报表的类型                             |  |  |  |  |
| 查询名称    |               | 此报表的名称                             |  |  |  |  |
| 所属部门    |               | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |  |  |  |  |
| 时间范围    |               | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |  |  |  |  |
| IP 地址范围 |               | 输入要查询的终端 IP 地址范围                   |  |  |  |  |
| 移动存储管理  | 审计筛           | 选择记录的审计内容,如删除、改名、创                 |  |  |  |  |
| 选       |               | 建等                                 |  |  |  |  |



#### 点击执行

| ALMAN (MI | #118.00   | 1000   | Ref.         | 828        | NH.                 |
|-----------|-----------|--|--------------|------------|---------------------|
| Mum PC    | 加速用       | 移动存取测数(Generic Fla<br>sh Disk V00 Device)    | HHRE         | ly.        | 2012/10/31 15:20:30 |
| UNLIN-PC  | 100EH     | 移动合理公室(Denient Fla<br>ah Diak USB Device)    | 語と名乗         | łę         | 2012/10/31 14:59:30 |
| Annue ES  | 同時用       | 移动存储设备(Generic File<br>sh Disk U(III Device) | <b>WITER</b> | ΤV.        | 2912/10/91 14:59:30 |
| LINE PC   | NU性用      | 移动仲積安璧(Damaric Fta<br>eh Diak い語 Device)     | IEX.89       | - br       | 2012/18/31 12:28:01 |
| Uium PC   | 1100年間    | 移动存储设备(Generic Fla<br>sh Daik USD Device)    | Not-27       | ly:        | 2012/10/91 12:20:01 |
| hanaan PC | noteHL    | 日己介護交換(Generic Pla<br>ah Diak USB Device)    | (E)/将章       | łw.        | 2012/10/31 12:13:82 |
| hasan PC  | mjärt     | 移动存储发展(Generic Fla<br>ah Disk USB Device)    | en or        | The second | 2012/10/31 12:13:32 |
| hinias.PC | molefill  | 包約仲保包盤(Danvinic Pla<br>sh Disk USB Device)   | 152.66       | θý.        | 2012/10/31 12:11:51 |
| nnum PC   | muiêril   | 移动存得安全(Generic File<br>sh Disk USB Device)   | en da        | he .       | 2012/10/31 12:11:51 |
| ansan.ec  | moterili. | 協会仲操役協(Generic Fla<br>ah Diak USB Device)    | <b>BINRS</b> | - N        | 2012/10/31 11:25:29 |

### 解扰审计

客户端移动存储设备进行分区表解扰时记录的审计信息



| 配置项:    | 说明                                 |
|---------|------------------------------------|
| 查询类型    | 此报表的类型                             |
| 查询名称    | 此报表的名称                             |
| 所属部门    | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 时间范围    | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| IP 地址范围 | 输入要查询的终端 IP 地址范围                   |
| 解扰审计筛选  | 选择记录的审计内容,如解扰、启动工具<br>等            |



#### 点击执行

| 10MM INSE | MURR          | Ren          | 采用的          | 務住.     | JA .  | -168        |
|-----------|---------------|--------------|--------------|---------|-------|-------------|
|           |               |              |              |         | W1/6  | 出来过的改善加     |
| 移动存储文     | (件审计          |              |              |         |       |             |
| 秋点型       | 移动存储文件审计      | F            |              |         |       |             |
| 服务名称      | 移动存储文件审       | +            |              |         |       |             |
| 前國部门      | 95 (m 68/11)  |              |              |         | • [   | 法罪部门        |
| 间边展       | a & F 7       | -            |              |         |       |             |
|           | O A           |              | ंग झ         |         | 1     | 1           |
| 9地址回到     |               |              |              |         |       |             |
| 文件名称      |               |              |              |         |       |             |
| 排文件名称     |               |              |              |         |       |             |
| 非关型       | 不指定           |              |              |         |       |             |
| 國状态       | 全局            |              |              |         |       |             |
| 24        | administrator |              |              |         |       |             |
|           | 保存并执行         | 保存           | 执行           | 10485   |       | 取消          |
|           |               |              |              |         |       |             |
| 配置项:      |               | 说明           |              |         |       |             |
|           |               |              |              |         |       |             |
| 报表类型      |               | 此报表的         | 类型           |         |       |             |
|           |               |              | <i>b 1 b</i> |         |       |             |
| 校衣名称      |               | 此报表的         | 名称           |         |       |             |
|           |               |              | 本治病          | 友 斗山 七亡 | 日山    | 5023 JA     |
| 新属部门      |               | 匹伴而安         | 宣调的圣         | 令师川     | 周的ì   | <b>部月,也</b> |
|           |               | 击 <b>"选择</b> | 部门" ∋        | 表进行     | 选择    |             |
|           |               |              |              |         | _ , , |             |
|           |               | 可选择最         | 近更新的         | 向天数     | 也可知   | 通过点击        |
| 时间范围      |               |              |              | ., .,,  |       |             |
|           |               | 图表选择         | 具体时间         | 訂范围     |       |             |
|           |               |              |              |         |       |             |
| P地址范围     |               | 输入要查         | 询的终站         | 耑 IP 均  | 也址范   | 围           |
|           |               |              |              |         |       |             |
|           |               | 选择记录         | 的审计团         | 内容,     | 如插    | 入、移除        |
| 操作类型      |               |              |              |         |       |             |
|           |               |              |              |         |       |             |

点击执行



| TRADIC            | ANAD SUP      | 3xna                   | HEADA                | B    | 86                                      | and<br>R | 100                     |
|-------------------|---------------|------------------------|----------------------|------|---|----------|-------------------------|
| 10.291.00.2       | kuyuan-<br>PC | H:\8980890908.<br>Dit  | H/8080800668.<br>bit | đk   | C/Window/Jaystem32\<br>WDDHost.exe      | 1        | 2012/10/31 9:5<br>3:58  |
| 10.201.96.2       | kuyuan-<br>PC | HI VOIDE               | Hind/bit             | 40   | CI/Windowslaystem32\<br>WUDFHost.ore    |          | 2012/10/31 9:5<br>3/50  |
| 18.381.50.2<br>13 | Boysam-<br>PC | HI VISIONOODOS.<br>Tot | HC/0580000008.       | dit: | CIVEndowPayaten32)<br>WUDFHostare       |          | 2012/30/38 14:5<br>9:27 |
| 10,291,90,2       | Toosum-<br>PC | H:Y0.bt                | Ht\0.txt             | #P   | C:\Windows\system32\<br>WUDFHost.exe    |          | 2912/10/30 14:5<br>9/27 |
| 10.201.00.2       | Bayuan-<br>PC | H:\8980890808.<br>txt  | H105900590808.<br>be | as.  | C:\//iii/dows/system32<br>WUDPHost.exe  |          | 2012/10/30 13:1<br>9:32 |
| 10.201.40.2       | kuyum-<br>PC  | HEVOLDE.               | Hill dat             | WER. | C/Windows/avaten375<br>WUDFHost.exe     |          | 2012/30/30 12:1<br>9:32 |
| 10.201.90.2       | huyuan.<br>PC | H URBOBOBOB.<br>Ed     | HORSEDEGERE.         | an   | C:\//indows/system32\<br>wUDPHost.ere   |          | 2012/10/30 12:1<br>8:22 |
| 10.201.90.2       | Ravan-<br>PC  | HIVD.DX                | HI/0.DIE             | an:  | C:///iindows/aysten/32\<br>WUDFHost.exe |          | 2012/30/30 12:1<br>8:32 |
| 10.201.00.2<br>13 | Buyuan-<br>PC | HI VERENDOOR           | H:\0000000000.<br>NC | 40   | C:\/IIindowi/Jaystan/37<br>WUDFHost.sos |          | 3613/30/30 43\3<br>#:32 |
| 10.2111.40.2      | kovum-<br>PC  | HI'W.bd                | HE'VO.IDH            | 读取   | C:\Windowslavstem32\<br>WUDFHost.exe    |          | 2912/30/30 12:1<br>8/32 |

# 15.10. 桌面运维

### 15.10.1. 配置介绍

| 请选择查询统计图表类型: | 🔘 终端资源使用状况告警查询   |
|--------------|------------------|
|              | ◎ 短消息阅读统计        |
|              | ◎ 指定终端短消息阅读查询    |
|              | ◎ 指定终端资源使用状况查询   |
|              | ◎ 终端网络累计使用状况TopN |
|              | 💿 计算机名规范查询       |
|              | ◎ 单点登录客户端查询      |
|              | 下一步 取消           |

终端资源使用状况查询需在"桌面运维"中配置"终端资源使用状

况监控与告警策略"

终端资源使用状况告警查询





| 配置项:  | 说明                                 |
|-------|------------------------------------|
| 报表类型  | 此报表的类型                             |
| 报表名称  | 此报表的名称                             |
| 所属部门  | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 主机名   | 输入要查询的终端主机名                        |
| 时间范围  | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围   |
| IP 地址 | 输入要查询的终端 IP 地址                     |
| 告警事件  | 选择告警事件,如 CPU 使用率、内存使用<br>率等        |

#### 点击执行

| No. of Lot of Lo | 主张构象          | INCOME.       | Man    | DMAG.    | 1.681.68            |
|--|---------------|---------------|--------|----------|---------------------|
| 10 201 340 22  | WIN-yangweie  | <b>Liga</b>   | 28%    | CPU使用生品智 | 2012/10/25 15:53:04 |
| 10.301 140.37  | WDe-yangweie  | ±®A           | 30.37% | 内存使用军击部  | 2012/10/25 13:33:64 |
| 10.203 100.27  | WBS-yangeene  | <u>_193</u> A | 38%    | 秘密制定空间击群 | 2012/30/25 15:53:04 |
| 10.201.140.22  | With yangwore | 二個A           | date   | 网络学校教会解  | 2012/10/25 15:33:04 |
| 10.201.140.27  | Wtheyangweie  | 2384          | 75.854 | 阿爾爾爾拉希爾  | 3013/10/25 15:53:04 |

#### 计算机名规范查询



| 报表类型        | 计算机名规范            | 查询             |                                      |              |              |
|-------------|-------------------|----------------|--------------------------------------|--------------|--------------|
| 报表名称        | 计算机名规范            | 查询             |                                      |              |              |
| 所属部门        | 所有部门              |                |                                      |              | 选择部门         |
| 计算机名长度      | 1                 | •              | 至 1                                  |              | 3),          |
| 域/工作组名称     |                   |                |                                      |              |              |
| 是否加入域       | 未指定               |                |                                      |              | •            |
| 创建状态<br>创建者 | 全局<br>administrat | or<br>Rat      | 执行                                   | mite         | THE CHE      |
|             | 11 JUL 1          | 1 1411         | 11941                                | dvirbu       | 40.41        |
| 配置项:        |                   | 说明             |                                      |              |              |
| 报表类型        |                   | 此查询的类          | 型                                    |              |              |
| 报表名称        |                   | 此查询的名          | 称                                    |              |              |
| 所属部门        |                   | 选择需要查<br>击"选择部 | 道的终端)<br>3 <b>门"</b> 来进 <sup>;</sup> | 所属的部门<br>行选择 | ],也可点        |
| 计算机名长度      |                   | 输入计算机          | 名的长度                                 |              |              |
| 域/工作组名称     |                   | 输入计算机          | 的工作组织                                | 或域名称         |              |
| 是否加入域       |                   | 选择是否加          | 1入域                                  |              |              |
| 计算机名规范告诉    | 2763              |                |                                      |              |              |
| iPieg INS   | <u> 68.65</u>     | 198            | H/ICENS                              | 1            | <u>460</u>   |
| 1           |                   |                |                                      |              | 月1页/共有1页0录数据 |

#### 指定终端资源使用状况查询

指定终端在一段时间内 cpu,内存,硬盘,网络数据包,字节数曲

#### 线图





| 报表类型  | 此报表的类型                           |
|-------|----------------------------------|
| 报表名称  | 此报表的名称                           |
| 时间范围  | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围 |
| IP 地址 | 输入要查询的终端 IP 地址                   |

点击执行







#### 终端网络累计使用状况 TopN

| 报表类型    | 终端网络累计使用状况TopN  |
|---------|---|
| 报表名称    | 终端网络累计使用状况Top10   |
| 所属部门    | 所有部门 → 选择部门   |
| 时间范围    | ◎ 最近 7 天  |
|         |   |
| IP地址范围  |   |
| 资源类型    | 收发数据包   |
| TopN    | 10  |
| 图表类型    | <ul> <li>无图</li> <li>) 讲状图</li> <li>() 横向柱状图</li> </ul> |
| 创建状态    | 全局  |
| 创建者     | administrator   |
|         | 保存并执行 保存 执行 删除 取消                                       |
| 配置项:    | 说明  |
| 报表类型    | 此报表的类型  |
| 报表名称    | 此报表的名称  |
| 所属部门    | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择                      |
| 时间范围    | 可选择最近更新的天数也可通过点击日期<br>图表选择具体时间范围                        |
| IP 地址范围 | 输入要查询的终端 IP 地址范围  |
| 资源类型    | 选择记录的审计内容,如收发数据包、收<br>发字节数等                             |
| TOPN    | 输入要展现的终端数量  |
| 图表类型    | 选择图表类型,可选择" <b>饼状图"</b> 和"横<br>向柱状图"                    |

短消息阅读统计



| 报表类型        | 短消息阅读统                                  | i <del>l</del>         |                      |              |             |
|-------------|---|------------------------|----------------------|--------------|-------------|
| 报表名称        | 短消息阅读统                                  | iit                    |                      |              |             |
| 所属部门        | 所有部门                                    |                        |                      |              | ▼ 选择部门      |
| 创建日期        | <ul> <li>● 最近 7</li> <li>○ 从</li> </ul> |                        | 天<br>[]]] 到          |              |             |
| 短消息标题       | Ī                                       |                        |                      |              | <br>(可模糊查询) |
| 创建状态<br>创建者 | 全局<br>administrat                       | or                     |                      |              |             |
|             | 保存并执行                                   | ī 保存                   | 执行                   | 删除           | 取消          |
| 配置项:        |   | 说明                     |                      |              |             |
| 报表类型        |   | 此报表的类                  | 型                    |              |             |
| 报表名称        |   | 此报表的名                  | 称                    |              |             |
| 所属部门        |   | 选择需要查<br>击 <b>"选择部</b> | 询的终端<br><b>门"</b> 来进 | 所属的部门<br>行选择 | 门,也可点       |
| 创建日期        |   | 可选择最近<br>图表选择具         | 更新的天<br>体时间范         | 数也可通〕<br>围   | 寸点击日期       |
| 短消息标题       |   | 输入要查询<br>模糊查询          | 的已发布                 | 的短消息的        | 的标题,可       |

#### 指定终端短消息阅读查询

| 报表类型         | 指定终端距消息间含显得   |      |        |  |
|--------------|---------------|------|--------|--|
| 报表名称         | 描定终端把消息网续查询   |      |        |  |
| 9500001      | 所有部门          |      | - 送任部门 |  |
| BUTTER       | ● 推近 7<br>● 単 | Π N  | -      |  |
| Pittic       | 172.25.90.181 |      |        |  |
| 的建物态         | 全間            |      |        |  |
|              | 保存并执行 保有      | kfi  | 制除 取消  |  |
|              |               |      |        |  |
| 配置项:         | 说明            |      |        |  |
| 配置项:<br>报表类型 | 说明 此报:        | 表的类型 |        |  |



|       | 选择需要查询的终端所属的部门,也可点    |  |  |  |  |
|-------|-----------------------|--|--|--|--|
| 所馮即门  | 击" <b>选择部门"</b> 来进行选择 |  |  |  |  |
|       | 可选择最近更新的天数也可通过点击日期    |  |  |  |  |
| 创建口别  | 图表选择具体时间范围            |  |  |  |  |
| IP 地址 | 输入要查询的终端 IP 地址        |  |  |  |  |

单点登录客户端查询

| 报表类型     | 单点登录客户端董      | 8         |    |    |      |
|----------|---------------|-----------|----|----|------|
| 报表名称     | 单点登录客户满查      | <u>نا</u> |    |    |      |
| 新屬部门     | 所有部门          |           |    |    | 选择部门 |
| 是否自用单点登录 | 不指定           |           |    |    |      |
| 创建状态     | 全開            |           |    |    |      |
| 创建者      | administrator |           |    |    |      |
|          | (             |           |    |    |      |
|          | 译存并执行         | 保存        | 执行 | 副除 | 取消   |

| 配置项:     | 说明                                 |
|----------|------------------------------------|
| 报表类型     | 此报表的类型                             |
| 报表名称     | 此报表的名称                             |
| 所属部门     | 选择需要查询的终端所属的部门,也可点<br>击"选择部门"来进行选择 |
| 是否启用单点登录 | 可选择"不指定""不启用""启用"                  |

## 15.11. 级联报表

### 15.11.1. 配置介绍

查询在系统级联中,下级单位向上级单位上报的报表,以便上级单 位系统管理员能够了解其下级单位的情况,包括终端发现、操作系 统统计、主机类型统计、补丁安装信息。安全基线违规终端统计



#### 级联报表

| 级联报表         |                    |
|--------------|--------------------|
| 请选择查询统计图表类型: | ◎ 终端发现_级联报表        |
|              | ◎ 资产信息_操作系统统计_级联报表 |
|              | ◎ 资产信息主机类型统计_级联报表  |
|              | ◎ 补丁安装信息_级联报表      |
|              | ◎ 安全基线违规终端统计_级联报表  |
|              | ◎ 策略分发统计_级联报表      |
|              | 下一步 取消             |

比如点击"终端发现\_级联报表",进入查询页面

| 报表类型 | 终端发现_级联报表     |    |    |      |
|------|---------------|----|----|------|
| 报表名称 | 终端发现_级联报表     |    |    |      |
| 所属单位 | 天珣则试增强身份高级版   |    | 79 | 选择单位 |
| 创建状态 | 全局            |    |    |      |
| 创建者  | administrator |    |    |      |
|      | 保存并执行保存       | 执行 | 删除 | 取消   |
|      |               |    |    |      |

| 配置项: | 说明                 |
|------|--------------------|
| 报表类型 | 此报表的类型             |
| 报表名称 | 此报表的名称             |
| 所属单位 | 选择需要查询的单位,也可点击"选择单 |
|      | 位"来进行选择,以来查询该单位的报表 |

点击"执行"后

| <u>终端无限 级数报表</u><br>成选集集 |      |        |        |               |         |       |  |  |
|--------------------------|------|--------|--------|---------------|---------|-------|--|--|
| *12 2.18                 | Enan | 6169.9 | 202058 | <b>非空行的</b> 權 | 6.6.6.9 | 26M69 |  |  |
| R.R.W.C                  | 126  | 35     | 33     | 93            | 19      | 14    |  |  |
| 10 201 12 24             | 0    | 0      | 0      | α             | 0       | 0     |  |  |
| 10.201.91.211            | 28   | 38     | 1      | 19            | 8       | 1     |  |  |
| 高計                       | 1.46 | 53     | 34     | 132           | 19      | 35    |  |  |

其他查询报表的配置也类似这样

**注意**: 直属单位的终端数量就是本级单位的终端数量,下级单位(如 "天河办事处")的终端数量就是下级与其所有间接下级(下级的 下级到最下一级)终端数量和,其他数字和报表的数字也是这样理



解

## 16. 系统维护

## 16.1.关于系统维护

- "系统维护"确保了系统能够正常、高效运行。
- "系统日志"为管理员提供了管理的可追溯性。更重要的是,系
   统日志反馈"系统维护"的配置是否合理。
- "license 管理"通过 web 页面显示出用户授权信息,包括此 license 到期时间、相应功能模块和目前已使用的 license 授权数 量等信息。

## 16.2.系统维护

16.2.1. 客户端升级配置页面

### 配置介绍


| 客户端升级      |                 |                                |                     |                |                 |           |  |
|------------|-----------------|--------------------------------|---------------------|----------------|-----------------|-----------|--|
| 策略名称       | upgrade         |                                |                     | *              |                 |           |  |
| 策略描述       |                 |                                |                     |                |                 |           |  |
|            |                 |                                |                     | ÷              |                 |           |  |
|            | 客户端版本在:         | 66930000                       | (含)至 <sup>61</sup>  | 6940001        | *间,执行升级         |           |  |
|            | ☑ 禁止弹出重,        | 启提示框                           |                     |                |                 |           |  |
|            | □ 禁止安装检测        | 则提示                            |                     |                |                 |           |  |
|            | 🔲 使用延迟升级        | 级方式 (重启后禄                      | <b>替</b> 换)         |                |                 |           |  |
|            | 🔲 使用客户端         | 升级包升级(upd                      | laterun)            |                |                 |           |  |
| 生效时间       | ◉ 所有时间 (        | り 工作时间 〇                       | 非工作时间               | ◎ 以下时间         | æ               |           |  |
|            | 开始              | 时间                             | 结束                  | 时间             | 编辑删除            |           |  |
|            | 2012-03-10      | 9:00                           | 2012-03-1           | 0 13:30        | 漆加              |           |  |
| 在线模式       | 🗹 在线时生效         | ☑离线时生效                         | ģ                   |                |                 |           |  |
| 策略应用对象     | 查看及编辑           |                                |                     |                |                 |           |  |
| 创建类型       | 全局              |                                |                     |                |                 |           |  |
| 创建者        | jing            |                                |                     |                |                 |           |  |
| 注:右边有*号的项( | 目必须输入。<br>保存 删除 | 取消                             |                     |                |                 |           |  |
| 配置项:       |                 | <u>说明</u>                      |                     |                |                 |           |  |
| 策略名称       |                 | 输入合                            | ·适的策·               | 略名称,           | 以方便管理           | 0         |  |
| 说明         |                 | 用以说                            | 用以说明升级历史记录信息,以方便管理。 |                |                 |           |  |
| 客户端版本      | 客户端版本版本         |                                |                     | 升级策略有效的客户端版本范围 |                 |           |  |
| 林小兴山寺      | 如果选             | 如果选择,升级后不会提示用户重启。该参数           |                     |                |                 |           |  |
| 祭止理出里      | 不支持             | 不支持 66930000 版本以下的客户端。         |                     |                |                 |           |  |
|            |                 | 勾选后                            | 即使客                 | 户端有启           | 目动 360 安全       | 卫士时也不     |  |
| 林中安准桥      | 测报示             | 今再通                            | 山提示                 | 柝 该轰           | <b>数</b> 不支持 66 | 930000 版木 |  |
| MILX ACTU  |                 | □ △ 开开田远小悟。 以罗奴小义讨 00530000 版本 |                     |                |                 |           |  |
|            |                 | 以下的                            | 客户端。                | þ              |                 |           |  |
| 1          |                 | 1                              |                     |                |                 |           |  |

 禁止安装检测提示
 会再弹出提示框。该参数不支持 66930000 版本<br/>以下的客户端。

 使用延迟升级方式
 强制使客户端在重启后才进行升级。该参数不<br/>支持 66930000 版本以下的客户端。

 使用客户端升级包升级
 选择此项后,前面三项配置会均会失效,采用<br/>客户端 updaterun.exe 的方式升级

 应用到 IP 组
 点击"查看及编辑"超链接,选择指定的 IP 组、



工作组、主机名。

### 配置要点

6693升级可以采用2种方式:

方法一:保留原有的升级方式,即将客户端升级包改名成为 updaterun.exe 放在服务器安装目录下的 updateNT 目录中,配置升级 策略.

| C. SHITLANDAR             | Contraction in the            | AT C SEE         | 8.4 meta |  |  |
|---------------------------|-------------------------------|------------------|----------|--|--|
| 客户端升级                     |                               |                  |          |  |  |
| 最略名称                      | 1                             |                  |          |  |  |
| 單略描述                      |                               | -                |          |  |  |
|                           |                               |                  |          |  |  |
|                           | 客户端版本在:1                      | (含)至 66940001    | *词、执行升级  |  |  |
|                           | 口禁止伸出重直接示症                    |                  |          |  |  |
|                           | 口就止安装给消费所                     |                  |          |  |  |
|                           | 目使用证证并且为此。通道                  | 后發進)             |          |  |  |
|                           | 团 使用容户端升级包升级(                 | updaterun)       |          |  |  |
| 生效时间                      | ● 所有时间 ○ 工作时间 ○ 非工作时间 ○ 以下时间的 |                  |          |  |  |
|                           | 开始时间                          | 结束时间             | 1966 MIS |  |  |
|                           |                               | 2012-03-10 10:00 | 添加       |  |  |
| 在线模式                      | Dimeters Dimeter              | 1.0              |          |  |  |
| 前略应用对象                    | 《还没有应用到任何对象》                  | 重重及情報            |          |  |  |
|                           |                               |                  |          |  |  |
| 创建共型                      | 全局                            |                  |          |  |  |
| 的建共型<br>创建者               | 全周<br>jing                    |                  |          |  |  |
| 创建共型<br>创建者<br>主:右边有+号的项目 | 全局<br>jing<br>18须输入。          |                  |          |  |  |

方法二: 不需要使用客户端 patch 包。配置升级策略后,客户端自 动在后台通过和服务器的通信进行升级,配置如下:



| 各户端升级配置      | 自动卸载客户端                      | 数据库自动维护         | 软件分         | 发IP组网步         |
|--------------|------------------------------|-----------------|-------------|----------------|
| 客户端升级        |                              |                 |             |                |
| 策略名称         | 1                            |                 | -           |                |
| 196 August   |                              |                 |             |                |
|              | 容戶端版本在 1                     | (含)至 665        | -<br>240001 | •阈.执行升级        |
|              | □ 禁止弹出重扁提;                   | R HE            |             |                |
|              | □ 禁止對装检测提示                   | R               |             |                |
|              | 🗌 使用延迟升级方式                   | ま(重良后替挨)        |             |                |
|              | □ 使用客户端升级图                   | 5升级 (updaterum) |             |                |
| 生动时间         | <ul> <li>新有时间 ① I</li> </ul> |                 | )以下时间<br>1日 | 2<br>4541 with |
|              | (2010-00-10(0))              | 0               | 0(09930     | 运加             |
| 在线模式         | Diasian Di                   | 8/8/12:0        |             |                |
| 策略应用对象       | 《还没有应用到任何                    | 对意》重查及情感        |             |                |
| 的建美型         | 全局                           |                 |             |                |
| 862 <b>4</b> | jing                         |                 |             |                |
| E:右边有+书的项目   |                              | 6:0             |             |                |

**说明**:大多数客户端升级涉及到客户端驱动升级,可能需要重启操作 系统。

# 16.2.2. 自动卸载客户端页面







| 配置项:   | <u>说明</u>                                      |  |  |  |
|--------|--|--|--|--|
| 策略名称   | 输入合适的策略名称,以方便管理。                               |  |  |  |
| 策略描述   | 用以说明升级历史记录信息,以方便管理。                            |  |  |  |
| 生效时间   | 可以选择"所有时间""工作时间""非工作时<br>间""以下时间段"生效"开始时间"以及"结 |  |  |  |
| 王双时间   | <b>束时间"</b> 仅对"以下时间段"有效。                       |  |  |  |
| 策略应用对象 | 点击"查看及编辑"超链接,选择指定的 IP 组、                       |  |  |  |
|        | 工作组、主机名,立即触发客户端自动卸载。                           |  |  |  |

**说明:** 客户端卸载功能无需任何版本信息,V6691 以上版本均支持 该功能。

#### 配置要点

1、 点击"添加"自动卸载客户端策略,如下图:

| 自动卸载客户端      |                           |            |
|--------------|---------------------------|------------|
| 策略名称         | test                      | *          |
| 策略描述         | 自动卸载客户端                   | *          |
|              |                           | *          |
| 生效时间         | ◉ 所有时间 ◎ 工作时间 ◎ 非工作时间 《   | 〇以下时间段     |
|              | 开始时间 结束                   | 时间 编辑 删除   |
|              | 2012-03-10 9:00 2012-03-1 | 0 13:30 添加 |
| 在线模式         | ☑在线时生效 ☑离线时生效             |            |
| 策略应用对象       | (还没有应用到任何对象) 查看及编辑        |            |
| 创建类型         | 全局                        |            |
| 创建者          | jing                      |            |
| 注:右边有*号的项目必须 | 版输入。<br>【保存】 取消           |            |

2、点击策略应用对象"查看及编辑"超链接,选择指定的 IP 组、工作组、主机名。客户端获得改规则后,立即触发客户端自动卸载。



| 自动卸载客 | 户端                    |                   |                  |                |
|-------|-----------------------|-------------------|------------------|----------------|
| 对象类型  | IP组                   | ← 全部选中            |                  |                |
| 对象选择  | 1F组<br>工作组<br>主机名<br> | 254. x            | 90<br>172.25.1.* | 140 110        |
|       | 222                   | 🔲 172.25.1.110-pc | 172. 25. 22      | 172. 25. 85. 1 |
|       | 42                    | 99100             |                  |                |
|       | 确定                    | 取消                |                  |                |

### 16.2.3. 数据库自动维护

"数据库自动维护"的三种策略均含其他策略,只需配置任一策略即可。

- "数据库自动维护"通过"压缩数据库"提高系统运行效率。
- "数据库自动维护"通过"备份数据库"以备份系统审计数据。
- "数据库自动维护"通过"清除数据库"清除过期审计数据释放 磁盘空间。
- "备份数据库"策略首先对过期数据清除,然后备份原有数据库, 最后压缩数据库以节省空间,故配置备份数据库后不需要配置
   "清除数据库"。
- "清除数据库"不需备份原有数据,适合对审计数据不敏感的环境中使用。
- "压缩数据库"前系统将自动清除超出保留数据月的数据。

#### 压缩数据库页面

#### 配置介绍

| 客户端升级配置 | 自动卸载客户端             | 数据库自动维护 | 软件分发IP组同步 |
|---------|---------------------|---------|-----------|
| 数据库自动维持 | ŀ                   |         |           |
| 任务名称    | 压缩数据库               |         |           |
| 保留数据月数  | 3个月                 |         |           |
| 维护动作    | 压缩                  |         |           |
| 是否启用    | ◎是 <mark>◎</mark> 否 |         |           |
|         | 保存取消                |         |           |



| 配置项:   | <u>说明</u>                 |
|--------|---------------------------|
| 任务名称   | 压缩数据库,建议不要更改。             |
| 保留数据月数 | 压缩数据库同时会删除保留数据月以前的数<br>据。 |
| 是否启用   | 如果选择为"是",则数据库压缩策略生效。      |

#### 配置要点

1、 点击"压缩数据库"策略超链接,进入配置页面,如下图:

| 客户端升级配置 | 自动卸载客户端 | <u> 数据库自动维护</u> | 软件分发IP组同步 |
|---------|---------|-----------------|-----------|
| 数据库自动维持 | ĥ       |                 |           |
| 任务名称    | 压缩数据库   |                 |           |
| 保留数据月数  | 1个月     | •               |           |
| 维护动作    | 压缩      |                 |           |
| 是否启用    | ◎是 ◎否   |                 |           |
|         | 保存取消    |                 |           |

2、选择"保留数据月数"的下拉列表框,如下:

| 客户端升级配置      | 自动卸载客户端                                       | <u>数据库自动维护</u> | 软件分发IP组同步 |
|--------------|---|----------------|-----------|
| 数据库自动维护      |   |                |           |
| 任务名称         | 压缩数据库   |                |           |
| 保留数据月数       | 1个月   | •              |           |
| 维护动作<br>是否启用 | <u>1个月</u><br>2个月<br>3个月<br>4个月<br>5个月<br>6个月 |                |           |

3、点击"是否启用"该策略为"是",保存:

| 客户端升级配置 | 自动卸载客户端 | <u> 数据库自动维护</u> | 软件分发IP组同步 |
|---------|---------|-----------------|-----------|
| 数据库自动维护 | 1       |                 |           |
| 任务名称    | 压缩数据库   |                 |           |
| 保留数据月数  | 1个月     | •               |           |
| 维护动作    | 压缩      |                 |           |
| 是否启用    | ◎是 ◎否   |                 |           |
|         | 保存取消    |                 |           |

#### 清除数据库页面



备份。

# 配置介绍

| 客户端升级配置                           | 自动卸载客户端   | 数据库自动维护   | 软件分发IP组同步       | )         |
|-----------------------------------|---|-----------|-----------------|-----------|
| 数据库自动维持<br>任务名称<br>保留数据内数<br>维护动作 | 斉院教授庫<br>1介月<br>-<br>-<br>-<br>-<br>-<br>-<br>-<br>-<br>-<br>-<br>-<br>-<br>- |           |                 |           |
| 配置项:                              | ○是 ●否<br>保存 取済  | <u>说明</u> |                 |           |
| 保留数据月                             | 数   | 直接删除"保    | <b>留数据月"</b> 以前 | 的数据但不压缩,不 |

#### 配置要点

1、 点击"**清除数据库"**策略超链接,进入配置页面,如下图:

| 客户端升级配置 | 自动卸载客户端 | <u>数据库自动维护</u> | 软件分发IP组同步 |
|---------|---------|----------------|-----------|
| 数据库自动维持 | 户       |                |           |
| 任务名称    | 清除数据库   |                |           |
| 保留数据月数  | 3个月     | •              |           |
| 维护动作    | 清除      |                |           |
| 是否启用    | ◎是 ◎否   |                |           |
|         | 保存取消    |                |           |

2、选择"保留数据月数"的下拉列表框,如下:

| 客户端升级配置      | 自动卸载客户端                                | <u> 数据库自动维护</u> | 软件分发IP组同步 |
|--------------|--|-----------------|-----------|
| 数据库自动维护      |  |                 |           |
| 任务名称         | 清除数据库                                  |                 |           |
| 保留数据月数       | 3个月                                    | •               |           |
| 维护动作<br>是否启用 | 1个月<br>2个月<br>3个月<br>4个月<br>5个月<br>6个月 |                 |           |

3、点击"是否启用"该策略为"是",保存:



| 客户端升级配置 | 自动卸载客户端 | 数据库自动维护 | 软件分发IP组同步 |
|---------|---------|---------|-----------|
| 数据库自动维护 |         |         |           |
| 任务名称    | 清除数据库   |         |           |
| 保留数据月数  | 3个月     | •       |           |
| 维护动作    | 清除      |         |           |
| 是否启用    | ◎是◎否    |         |           |
|         | 保存取消    |         |           |

### 备份数据库页面

### 配置介绍

| 客户端升级配置    | 自动卸载客户端                 | <u> 数据库自动维护</u>  | 软件分发IP组同步   |
|------------|-------------------------|------------------|-------------|
| 数据库自动维     | þ                       |                  |             |
| 任务名称       | 备份数据库                   |                  |             |
| 保留数据月数     | 1个月                     | •                |             |
| 维护动作       | 备份                      |                  |             |
| 备份路径       | \\10.201.1.204\shar     | e 格式:\\192.168   | .0.2\share  |
| *请输入,用户名(包 | ]括域),格式:192.168.0.2\adm | inistrator (确认拥有 | 有该以上路径的写权限) |
| 用户名        | 10.201.1.204\admini     | sti              |             |
| 密码         | •••••                   |                  |             |
| 是否启用       | ◎是 ◎否                   |                  |             |
|            | 保存取消                    |                  |             |

| 配置项:   | <u>说明</u>                     |  |
|--------|-------------------------------|--|
| 保留数据月数 | 数据备份后系统会自动清除"保留数据月数"<br>前的数据。 |  |
| 备份路径   | 数据以示例格式备份。备份文件夹不支持中文。         |  |
| 用户名    | 具有写入共享文件夹权限的系统用户              |  |

### 配置要点

1、 点击"备份数据库"策略超链接,进入配置页面,如下图:



| 客户端升级配置     | 自动卸载客户端                 | <u> 数据库自动维护</u>  | 软件分发IP组同步  |
|-------------|-------------------------|------------------|------------|
| 数据库自动维护     | à                       |                  |            |
| 任务名称        | 备份数据库                   |                  |            |
| 保留数据月数      | 1个月                     | •                |            |
| 维护动作        | 备份                      |                  |            |
| 备份路径        | \\10.201.1.204\share    | 格式:\\192.168.0.  | 2\share    |
| *请输入,用户名(包: | 活域),格式:192.168.0.2\admi | nistrator (确认拥有) | 该以上路径的写权限) |
| 用户名         | 10.201.1.204\adminis    | sti              |            |
| 密码          | •••••                   |                  |            |
| 是否启用        | ◎ 是 ◎ 否                 |                  |            |
|             | 保存取消                    |                  |            |

2、选择"保留数据月数"的下拉列表框,如下:

| 客户端升级配置      | 自动卸载客户端 数             | 据库自动维护          | 软件分发IP组同步  |
|--------------|-----------------------|-----------------|------------|
| 数据库自动维护      |                       |                 |            |
| 任务名称         | 备份数据库                 |                 |            |
| 保留数据月数       | 1个月 🗸                 |                 |            |
| 维护动作         | 1个月<br>2个月            |                 |            |
| 备份路径         | 3个月<br>4个月            | 格式:\\192.168.0. | 2\share    |
| *请输入,用户名(包括的 | 5个月<br>6个月            | strator (确认拥有该  | {以上路径的写权限) |
| 用户名          | 10.201.1.204\administ | r               |            |
| 密码           | •••••                 |                 |            |
| 是否启用         | ◎是 ◎否                 |                 |            |
|              | 保存 取消                 |                 |            |

- 3、填写备份路径和用户信息。
- 4、点击"**是否启用"**该策略为"**是**",保存:

| 客户端升级配置    | 自动卸载客户端                 | <u> </u>         | 软件分发IP组同步  | 7 |
|------------|-------------------------|------------------|------------|---|
| 数据库自动维持    | 户                       |                  |            |   |
| 任务名称       | 备份数据库                   |                  |            |   |
| 保留数据月数     | 2个月                     | -                |            |   |
| 维护动作       | 备份                      |                  |            |   |
| 备份路径       | \\10.201.1.204\shar     | ◎ 格式:\\192.168.0 | ). 2\share |   |
| *请输入,用户名(包 | 括域),格式:192.168.0.2\admi | inistrator (确认拥有 | 该以上路径的写权限) |   |
| 用户名        | 10.201.1.204\admini:    | sti              |            |   |
| 密码         | •••••                   |                  |            |   |
| 是否启用       | ●是 ◎否                   |                  |            |   |
|            | 保存取消                    |                  |            |   |



# 16.2.4. 软件分发 IP 组同步

■ 软件分发 IP 组对象未出现时请使用该维护项,维护时已建立的 软件分发策略将被删除。

| 皆尸'病; | <b>开</b> 级官(五   | 目初即執各尸病                     | <b>烈</b> 撒 年 目 初 雅 伊 | <u> 软件分友中组</u> |
|-------|-----------------|-----------------------------|----------------------|----------------|
| 说明    | 软件分发IP<br>顶,维护时 | 组对象未出现时请使用该。<br>P建立的软件分发策略将 | <u>帮助</u><br>维护      |                |
|       | 除。              |                             | NX103                |                |

# 16.3. 系统日志

## 16.3.1. 管理员操作日志页面

"管理员操作日志":记录了日志时间、管理员、操作、对象、

详细信息,并提供了删除功能。

| nga   | C noter Gan             | 14  | 3 (84)         |             | 1    |
|---|-------------------------|-----|----------------|-------------|------|
| 201   | 225                     | 80  | 628            |             | 19.1 |
| 12/12/2012 1.101 00 19  | address of the states   |     | 管理性治病          | 17.03.06    | 893  |
| 1221/2012 1 00:09 74  | where strawe            | 199 | <b>安然</b> 在14林 | 100003      | 821  |
| 1.710/mill 1.95-94 98   | - address to track as   | 378 | WRIT           | 100040      | 803  |
| United to be an an  | advector state          | 82  | 88727          | (Alasta for | 801  |
| 1/15/0012 1.09.20.09  | adulationeration        | 2.0 | VIDINAR        | (THEAR      | 812  |
| U.S. MARKER A. M. DE M.   | addition of earlier     | 8.0 | WETHE          | (Based by   | 822  |
| 1/10/0001 1-00-10-00  | address of realists     | 214 | WRALIN         | 10000       | 493  |
| 121220011110100   | electricity environment | 8.2 | *****          | 10000       | 102  |
| and the second se |                         |     |                |             |      |

**说明**:三权分立版本中,审计员的操作只能由帐号管理员查看和删除。 帐号管理员操作由审计员查看和删除。

"详细信息":对系统操作的行为记录,以 SQL 语句的形式记录,如下:



| - 211Riu                 | AAHESA-        | - 7604 | 0.22580      | 3 esta 3 mm  | - |
|--------------------------|----------------|--------|--------------|--|---|
| 111                      |                | 85     | A Reserve    | 17 Page  | - |
| 14/15/09/2               | allegeneration | 1899   | \$27.04      | dena R   | 1 |
| 11/12/2011               | abiaistate     | 13.00  | WEG HA       | (Failth)   | 1 |
| 10/10/0010<br>10:10.10   | alministratio  | da:    | 881          | HERRY 1007 DEL Super-Desentante esta effectives, articles et al. (a) establish prevalution reserved,<br>interested, resta effectives (h), filteration, filteration, filteration, constant of any other<br>endoarders, articulations, establish, interchlored (MART)<br>(h), project, 11, 21, 51, 51, 64, 64, 64, 95, 66, 66, 66, 67, 67, 68, 68, 68, 68, 68, 68, 68, 68, 68, 68  |   |
|                          | whereinsteine  | 80     | -            | 1013   | 1 |
| 1111/1012<br>1011/1012   | abistetesta    | un.    | <b>BOURK</b> | 1011   | 1 |
| 10/10/2011<br>10:20 (%   | abiatiteste    | 88     | -            | and a second sec |   |
| 10/15/0011<br>1.25.11.15 | adalactivator  | 28     | ***          | (chan  | 1 |
| ALL OF THE               | abisotote      | 92     | \$267,82     | 44838  |   |

## 16.3.2. 按需支援日志页面

"按需支援日志":记录了管理员 IP 地址、管理员登录名、客户

端 IP 地址等。



**说明:** 三权分立版本中,按需支援管理员由系统操作员创建和维护。 按需支援管理员无删除操作日志的权利,操作日志有系统操作员删 除。

#### 15.2.3策略服务器日志页面

"策略服务器日志":记录了策略网关代理、RADIUS 服务器、
 ES 软件分发服务等启动、取策略的行为,以及客户端取策略和
 发送报表的行为。



| 教授关系的主         | 検索支援日志 | MARS SHE   | 重新音樂權务證明多日志     | 業時间关日志 | RADIUSEI & | 种丁则多日志 |
|----------------|--------|------------|-----------------|--------|------------|--------|
| 策略服务器日志        | ř.     |            |                 |        |            |        |
|                |        |            |                 | 塑炼     |            |        |
| <b>济和</b> 人日期  | 植式古日   | 田中的白袍,北北口, | 如果不能入日期,就重要所有的日 | 志*     |            |        |
| - 曲达探解範疇充著     |        |            |                 |        |            |        |
| <b>查后服务器日志</b> | 1      |            |                 |        |            |        |

"策略服务器日志"以 TXT 文档格式提供查看,如下图:

| Server_Log.txt - 记事本   |   |  | × |
|--|---|--|---|
| 文件(F) 编辑(E) 格式(O)  | 查看(V) 帮助(H)   |  |   |
| $\begin{array}{c} 2012-11-13 & 13:29:47\\ 2012-11-13 & 13:30:25\\ 2012-11-13 & 13:30:35\\ 2012-11-13 & 13:33:10\\ 2012-11-13 & 13:38:09\\ 2012-11-13 & 13:47:26\\ 2012-11-13 & 14:05:16\\ 2012-11-13 & 14:05:22\\ 2012-11-13 & 14:09:50\\ 2012-11-13 & 14:09:50\\ 2012-11-13 & 15:14:23\\ 2012-11-13 & 15:14:23\\ 2012-11-13 & 15:14:24\\ 2012-11-13 & 15:14:24\\ 2012-11-13 & 15:14:25\\ 2012-11-13 & 15:14:25\\ 2012-11-13 & 15:14:25\\ 2012-11-13 & 15:14:27\\ 2012-11-13 & 15:14:27\\ 2012-11-13 & 15:28:17\\ 2012-11-13 & 15:28:17\\ 2012-11-13 & 15:31:40\\ 2012-11-13 & 15:31:40\\ 2012-11-13 & 15:34:28\\ 2012-11-13 & 15$ | $\begin{array}{c} 10, \ 201, \ 1, \ 204\\ 10, \ 201, \ 1, \ 204\ 10, \ 201, \ 1, \ 204\ 10, \ 201, \ 1, \ 204\ 10, \ 201, \ 1, \ 204\ 10, \ 201, \ 1, \ 204\ 10, \ 201, \ 1,$ | 服插 R 服 A 指插插插插插插插插插插插插插插 R R A 插插件件件件件件件件件件件件件件件件件 | E |
| L.   |   |  |   |

# 15.2.4告警服务器同步日志页面

"查看策略服务器同步日志":记录了本地告警服务器和中心告

警服务器的同步信息。

| 管理资源作日本 | 研究交援日本 | 黨總備有書目之 | 查查查要要方言用自己主 | <b>新闻同</b> 关日本 | RADOUSEL | <b>补丁同参日</b> 集 |
|---------|--------|---------|-------------|----------------|----------|----------------|
| 告警服务器网  | 步日志    |         |             |                |          |                |
| -RANNER | ð- •   | 理题      |             |                |          |                |
| 2662842 | 用作日主   |         |             |                |          |                |

## 15.2.5策略网关日志页面

"策略网关日志":记录了未安装天珣客户端终端信息。



| 管理问题中日志         | 接重支援日本 | <b>第時股份</b> 2日志  | 重要改善服务者的全国主     | 國際民主 | RADIUSELE | #T <b>R</b> \$83 | 1 |
|-----------------|--------|------------------|-----------------|------|-----------|------------------|---|
| 蓥略同关日志          |        |                  |                 |      |           |                  |   |
| -               |        | DEADER Have      |                 | NE   |           |                  |   |
| 88/128          | Mar N  | NUMBER OF STREET | 但那个新人口般+ 把重着用用的 | 96*  |           |                  |   |
| -请法保某规问大!       | 18 .   |                  |                 |      |           |                  |   |
| <b>東南洋南阿</b> 米田 | £      |                  |                 |      |           |                  |   |

"策略网关日志": 以 TXT 文档格式提供查看,如下图:

| 🦳 Server_Log1.txt - 记事本  | 3 |
|--|---|
| 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)  |   |
| 文件() 編辑(E) 格式(O) 查看(V) 帮助(H)<br>2012-11-13 14:6:3 172.25.90.203没有运行策略系统<br>2012-11-13 14:9:32 10.201.100.13没有运行策略系统<br>2012-11-13 14:10:7 10.201.100.13没有运行策略系统<br>2012-11-13 14:14:16 10.201.100.13没有运行策略系统<br>2012-11-13 14:42:51 10.201.99.206没有运行策略系统<br>2012-11-13 14:43:7 10.201.99.206没有运行策略系统<br>2012-11-13 14:43:7 10.201.99.206没有运行策略系统<br>2012-11-13 14:43:73 10.201.99.206没有运行策略系统<br>2012-11-13 14:43:53 10.201.99.206没有运行策略系统<br>2012-11-13 14:43:53 10.201.99.206没有运行策略系统<br>2012-11-13 14:44:55 10.201.99.206没有运行策略系统<br>2012-11-13 14:44:55 10.201.99.206没有运行策略系统<br>2012-11-13 14:44:55 10.201.99.206没有运行策略系统<br>2012-11-13 14:44:55 10.201.99.206没有运行策略系统<br>2012-11-13 14:44:55 10.201.99.206没有运行策略系统<br>2012-11-13 14:45:10 10.201.99.206没有运行策略系统<br>2012-11-13 14:45:10 10.201.99.206没有运行策略系统<br>2012-11-13 14:45:10 10.201.99.206没有运行策略系统<br>2012-11-13 14:45:10 10.201.99.206没有运行策略系统<br>2012-11-13 14:45:27 10.201.99.206没有运行策略系统 | A |
| 2012-11-13 14:46:59 10.201.99.206没有运行策略系统<br>2012-11-13 14:46:59 10.201.99.206没有运行策略系统   |   |
| 2012-11-13 14:47:14 10.201.99.206没有运行策略系统  | - |
|  |   |

# 15.2.6RADIUS 日志页面

| EMAMPELLE HE            | AMELE          | ####D-8218   | ***           | edesest.     | INTER215    | KAODOREE | 112460 | #30%                                    |             |
|-------------------------|----------------|--|---------------|--------------|-------------|----------|--------|---|-------------|
| NADTOSILie日志            |                |  |               |              |             |          |        |   |             |
|                         |                |  | 3.0           |              |             |          |        |   |             |
| REGISTER Server         |                | and the state of t | 1.            |              |             |          |        |   |             |
| 0.580                   | 15 P           | anti-prise   | augue         |              |             |          |        |   |             |
| MARRIAL CO.             |                | for an increase  | 100 10 100    | 1110         |             |          |        |   |             |
| Again the second second | 100            |  |               |              |             |          |        |   |             |
| 61199 <b>0</b>          |                |  | 100.0         |              | 75          |          |        |   |             |
| LANGUM MIL              |                |  |               |              |             |          |        |   |             |
| DACES                   |                |  | -             | -            |             |          |        |   |             |
| 104106                  | 100            |  |               |              |             |          |        |   |             |
|                         |                |  |               |              |             |          |        |   |             |
| *111                    | 11.00          |  | COLUMN STREET | 000000       | 000000      |          |        | 000000000000000000000000000000000000000 | W100-30-077 |
| 1/1/1/10 11 14 18 19    | (Astronomical) | the state of the s | stand and     | 10.001.1.110 | MIC 1011/07 |          | X      | Akr.                                    | 1523        |
| 10/10/10 2:30:30 19     | 000000000      | ĸ  | weekeet and   | 10.001.1.110 | 00.0348     |          | 8      | RML                                     | Stick       |
| LAUNTER COLOR 19        | (constant)     | -  |               | 10.005.1.010 | 90.100.2    |          | *      | Rate.                                   | stah        |
| 11/1/1912 1 10:19 19    | 0000000.0      | K.   | susation.     | 10 189 1 118 | 401.11544   |          | 8      | RML                                     | (CU)        |
| 11/1/10110 0 19:08 28   | otherap        | e  | -reversed     | 10.001.1.110 | 00E 100/02  |          | *      | MAL                                     | 6171        |
| OVANIE E H M M          | ORONAL REPORT  |  | reported.     | 10 101-1 110 | an innt     |          | Ă.     | 3,41                                    | 60.5        |
| 11/0/1111 10:10:17:00   | 6834464        | 10   | 1986          | 10.001.1.111 | KNALE.      |          |        | diaries.                                | 852h        |
|                         |                |  |               |              |             |          |        |   |             |

"RADIUS 日志":记录了网络准入下客户端认证信息。

# 15.2.7补丁同步日志页面

"补丁同步日志":记录了补丁同步服务器与外网服务器同步的



| 详细信                       | 息,供补丁同步失败时查                 | 询。                |
|---------------------------|-----------------------------|-------------------|
| 被继续操作的支 拆录                | 支援日志 新時期外著日志 宣告內祭服外湯四多日志    | WRITHERS RADIUSES |
| 日本日本 第二                   | 1                           |                   |
| and the second second     |                             |                   |
| REAL PROPERTY AND INCOME. | MR.                         |                   |
| 10/31/2012 11:42:52 19    | 法考虑的重制计计管理系统                |                   |
| 10/31/2012 11:42:53 29    | 影响重要发布的外位重                  |                   |
| 10/31/0212 11:42 83.08    | EADERSHINE                  |                   |
| 10/01/2012 11:42 10:39    | 开始出来协能规则行了管理                |                   |
| 10/31/0312 11:40:53 (9)   | 演奏内计信用成为内部                  |                   |
| 10/31/2010 11:40:10:19    | 查找外经复用步动乘 我的V学协定算,01次件委费下载/ |                   |
| 10/31/2010 11:40 10:10    | NIX-12-DIRECTION-CIT        |                   |
| 10/11/0112 11:42 49 78    | 的基于使爱达里                     |                   |
| 10/31/0310 11:40 49-89    | 和中计工机总统规则                   |                   |
| 10/35/2012 11:42:49.08    | 积冲得于40.7%或功,正在处理绘制          |                   |
| 10/01/0022 11:42:48:39    | 他的时间了AII周围来放                |                   |
| 10/31/0812 11 42:40 29    | 病毒药症的过去分娩;此此                |                   |
| 10/11/2012 11:42:40 29    | 病毒药管理成素 YABADIN 正在处理性理      |                   |
| 10/31/0012 11:40:40 08    | 病毒药组织与法用多开始                 |                   |
| 10/11/2012 11:40:40 28    | <b>南等药提</b> 到会计解释实现         |                   |
| 10/10/2012 11:40:40:29    | 正在处理的问题的问题就                 |                   |
| 10/31/3012 11:40:40 08    | 病毒药建筑合理下和成功。正在处理阶级          |                   |
| 10/11/2012 11:42:40:10    | (1)的现象任务自动展示,自动现象任务场理成功)    |                   |
| 10/21/2012 11 42 49 19    | <b>W基苯甲的 开始</b>             |                   |
| 10/71/2012 11:42:40 PM    | 道水,四位十段更新任务。                |                   |
| 1121111220-               |                             |                   |

# 16.4. License 管理

#### 配置介绍

| <u>License管理</u>    | 授权客户端管理                                |
|---------------------|--|
| 产品授权信息<br>导入license | 导出license                              |
| 产品名称                | 天珣内网安全风险管理与审计系统                        |
| 授权单位                | 天珣测试高级版授权                              |
| 授权类型                | 正式授权,升级维护服务有效期截止到2013年9月30日!           |
| 授权IP                | 10, 201, 1, 204                        |
| 授权数量                | 1000                                   |
| 授权模块                | 基本模块<br>网络准入<br>终端审计<br>移动存储管理<br>桌面管理 |
| 当前授权客户端             | 35                                     |

| 配置项:       | <u>说明</u>        |  |
|------------|------------------|--|
| 导入 License | 从服务器管理界面导入天珣授权文件 |  |
| 导出 License | 从服务器管理界面导出天珣授权文件 |  |



| 产品名称    | 天珣内网安全风险管理与审计系统            |
|---------|----------------------------|
| 授权单位    | 使用单位                       |
| 授权类型    | 正式授权或试用授权                  |
| 授权 IP   | 授权的单位服务器 ip                |
| 授权数量    | 客户端授权的数量                   |
| 授权模块    | 天珣内网安全风险管理与审计系统当前授权的<br>模块 |
| 当前授权客户端 | 授权的客户端数量                   |

| 当前授权客户端                                      |                  |                       |   |                                  |          |
|--|------------------|-----------------------|---|----------------------------------|----------|
| 1718121                                      |                  | 9-10U                 | 20.8-                                   |                                  | 11       |
| 7((115))                                     |                  | 重調                    |   |                                  |          |
| a 900  | ALC: REAL        | TH: 182               | 186                                     | III GIRLAN                       | 124031   |
| C BESTER DOCTOR                              | 112 25 254 54    |                       | Rok-to-topal                            | 10/21/2012 1:15:23<br>78         | a.       |
| DATADISTO-MEET-                              | 10.218.110.206   | 00-40-40-37-40-<br>M  | ning2000284.tax teachour var 2003221112 | 10/01/2012 4:45 55               | 4        |
| D 10000001 1140-0000                         | 10 101 101 07    | 80-90-98-98-90-<br>75 | ALF TT                                  | 10/10/1018<br>12 00 38 <b>19</b> | R.C.     |
| D 120794039-1404-4011-<br>1000-5601800066617 | 112, 25, 04, 05  | 90-30-38-33-43-<br>Ck | niwnin                                  | 11/3/2012 10:36.36<br>#8         | 4        |
| C SERVICE COL                                | 10.201 30.117    | 00-02-29-38-99-<br>33 | ROM-RECEDUTIONS                         | 10/25/2012 4:30-18<br>29         | £.       |
| DA001180-0717-6/21-<br>#521-14258/000781     | 10,205,306,17    | 00-00-29+08-08-       | jing/ue-MAsp                            | 20/29/0012.5130.41<br>85         | #):      |
| COMPLIANCE (COMPLIANCE COMPLEXING)           | 172 35 42 303    | 00-02-29-89-39-<br>70 | and Le 100 all de                       | 10/31/0012 3:06:01<br>19         | 4        |
| DECEMPTION NEWS                              | 30,259,222,96    | 00-04-30-31-36-<br>36 | Aur HT                                  | 507 3672012<br>10: 59: 15: 46    | <u>.</u> |
| C (MOLINO)-EAST-ADE-                         | 10, 501, 502, 77 | 00-00-00-00-00-<br>M  | FIR-SHELFORIDA!                         | 39/15/1912 3.57.48<br>29         | 8.       |
| D ROCATRON-SELE-GRO-<br>4251-DESEOPOTRAL     | 10 201 90 213    | 0C-82-63-37-60+<br>04 | Lowest C                                | 20/25/2012 2-54 29<br>78         | 1        |
| 1225   |                  |                       |   |                                  |          |

注意:删除选中的授权客户端只能删除当前不在线的客户端.

# 16 系统级联

# 16.1 关于系统级联





- 各个单位都部署有自己的策略服务器(一个中心服务器和0到多 个本地服务器),并且都有直属自己策略服务器管理的终端,不 同单位的中心服务器根据单位的从属关系进行互联,形成物理上 分层的多级架构。
- 上级能够选择性下发策略策略到所有下级服务器。下级接受到上级下发的策略后,仅仅只能关联下级所属的 IP 组下发到客户端,不能对上级下发的策略进行其他修改、删除等操作。
- 级联架构下支持仅使用唯一一个 license.dat 授权文件,并支持上级为下级服务器分配终端授权数量。

# 16.2 级联关系

# 16.2.1 配置介绍

拥有系统级联操作权限的系统管理员能在本级单位向上级单位发 起申请和确认下级单位的请求,从而建立上下级关系;没有权限的 管理员对级联关系页面只读。



| 望康关系   |               |
|--|---------------|
| 级联关系   | 帮助            |
| 上领单位:厂东省办事选(正常)  |               |
| □-本頜单位:广州办事处   | 修改单位名称        |
| - 学越秀办事处(等待确认)   | <u> 通认</u> 撤销 |
| □<br>示<br>「<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一<br>一 | 管理撤销          |

一个单位有零到一个上级单位,若还未添加上级,则可以点击"添 加上级",填入上级单位服务器的 IP 地址,保存后等待上级确认即 可。

| 添加上级单位        |   |
|---------------|---|
| 上级单位中心服务器IP地址 | 1 |
|               |   |

**注意**:在上级单位未对下级单位的请求确认之前,下级单位处于"提 交请求"或"等待确认"的状态时,下级单位可以将上级单位删除, 一旦上级单位确认请求,下级单位就不能将上级单位删除,只能由 上级单位撤销下级单位。

点击"修改单位名称",可以修改本级单位名称并同步到上下级

| 级联关系            |        |          |
|-----------------|--------|----------|
| 修改单位名称          |        | <u>0</u> |
| <b>本级</b> 里区石树  | 广东省办事处 | *        |
| 注:右边有*号的项目必须输入。 | 保存取消   |          |

一个单位可以有零到多个下级单位,对于下级单位向本级单位提出的请求,可以点击"确认"来建立关系,或者点击"撤销"来拒绝请求



对于已确认的下级单位,可以点击"管理"查看下级单位的策略和 报表,或者点击"撤销"来删除下级单位。(对于已分配授权的下 级服务器,上级是无法撤销该下级服务器的)

若下级单位被上级撤销了,下级单位(处于已被上级删除,如下图) 需要管理员在页面人工点击"**删除上级"**(已确保管理员能被通知 到上级已将本单位删除)



**注意**:要保持上下级单位服务器网络是可达的,并且只能由下级向 上级申请,上级对下级进行确认关系。下级单位名称的图标亮着表 示服务器在线。

# 16.3 级联策略管理

### 16.3.1 配置介绍

级联策略管理"页面,用于管理员选择和下发策略到下级。

| 鐵稅                   | 下发的策略   |                           |
|----------------------|---|---------------------------|
|                      | 11640.001612.11019900   | GLEE DETHNE CORLEE DETHNE |
|                      | *****   | NI                        |
|                      | 8-28-P  |                           |
|                      | *****   | 10.00                     |
|                      | *** 816   | State.                    |
|                      | 8-00-W  | 10.00                     |
|                      | dimenti   | sed.                      |
|                      | HTRM  | 無能                        |
| 的自己用利用               | (现没再应用到任何问题) 重新加速器  |                           |
| 「「「「」」               | ±8  |                           |
| IIRA                 | jug   |                           |
| EI THAF FINGE (FALL- | and the second se |                           |
|                      | <b>秋</b> 奈 和 <u>西</u>   |                           |

点"**编辑"** 



| 下发的策略       |                                  |
|-------------|----------------------------------|
|             | 在线和编线生动的频率 👥 位在线生动的策略 👥 位徽线生动的策略 |
| 安全基項        |                                  |
| -           |                                  |
| bbbb        |                                  |
| cocce       |                                  |
| E 66466     |                                  |
| Elses       |                                  |
| T HHH       |                                  |
| 00095       |                                  |
| E HOTOPHI   |                                  |
| Etestet     |                                  |
| Elter       |                                  |
| E test      |                                  |
| Thestorier1 |                                  |
| 📃 testeler2 |                                  |
| testrier3   |                                  |
| Retfix      |                                  |
| hotfin      |                                  |

"确认",该策略会下发至所有下级服务器。下级服务器只能应用

该策略,不能编辑,修改和删除该策略。

点击策略应用对象的"查看及编辑"

| 级联关系 | 级联策略管 | 里 🗋    | 授权分拆     | )  | 级联软件分发介质同 | 步 |
|------|-------|--------|----------|----|-----------|---|
|      |       |        |          |    |           |   |
| 下级单位 |       | 10.201 | .91.211  |    | -         |   |
| 应用对象 |       | ◎ 所有   | 对象 💿 指定; | 对象 |           |   |
| 对象类型 |       | 无      |          |    | •         |   |
|      |       |        |          |    |           |   |
|      |       | 确定     | 取消       |    |           |   |

应用对象可以选择"无""ip 组""工作组""主机名",选择"无" 表示取消全部下发策略,取消后,下级服务器可以进行编辑,修改 和删除。

如果在上级服务器删除某条已下发的策略,则下级服务器可以进行 编辑,修改和删除。

16.4 授权分拆

## 16.4.1 配置介绍

级联架构能够支持按照实际需求,将上级授权逐级向下分发授权数 量,并可以查看各级授权情况。



| 要联关系  | 服業業務管理 | 親致分革                                    |                       |      |        |      |      |
|-------|--------|---|-----------------------|------|--------|------|------|
| 产品授资  | (信息    |   |                       |      |        |      | 1    |
| 产品名   |        | ANDERSING                               | 的基本部计系统               |      |        |      |      |
| 便校典型  |        | 试用后来,2012年20                            | 用印日教師                 |      |        |      |      |
| 用户名   |        | Veux                                    |                       |      |        |      |      |
| 신하음   |        | Vena II.                                |                       |      |        |      |      |
| 部列号   |        | 1017-2079-0120-61                       | 10-1012               |      |        |      |      |
| 产品质权力 | ŧ.     | 100                                     |                       |      |        |      |      |
| 授权權法  |        | 基本组织<br>同時主人<br>約3年11<br>日均存制管理<br>点面管理 |                       |      |        |      |      |
| 使权分析  |        | ROCIENTE<br>CONSTRUCT<br>CONSTRUCT      | ∰: 47<br>1 10<br>1 43 |      |        |      |      |
|       |        | 单位起端                                    | 12.00.00              | **** | ERRICA | 動反抗進 | 编改图数 |
|       |        | 15 201 88 8                             | 10.201.85.8           | 18   | 1      | 日間台  |      |

授权分拆可以本级授权使用情况,及下级服务器的授权状态。 本级已注册终端数量:显示本级服务器已注册的终端数 已分配的授权数量:显示本级已分配给下级服务器的全部授权数量 可分配的授权数量:产品授权数量-(本级已注册终端数量+已分配 的授权数量)

点击"修改授权"笔形按钮可以对下级已分配的授权数量进行修改。 注意:修改授权数不允许小于已使用授权数。

# 16.5 级联软件分发介质同步

# 16.5.1 配置介绍

级联软件分发介质同步主要用来同步上级服务器 SDDownload 目录下文件夹 cascadeSD 的文件到下级服务器同样的目录下,在这个过程中,需要手动才能同步。

| DRXM  | CO. | BERC ST IN | SARTING STREET |            | _ |
|-------|---|------------|----------------|------------|---|
| 级联软件  | 分发介质同步发                                 | 日志豊適       |                |            |   |
| 3640  | 20                                      |            | - SOME         |            |   |
| 相同語   |   |            | Cl 31          | C OGATAABR |   |
| R#96  | 708                                     |            |                |            |   |
| 10.00 |   | 1141       | 63             | 43         |   |
| 3     |   |            |                |            |   |



注意:级联软件分发策略下发前需要先同步介质,否则,下 级策略在做 MD5 摘要校验时,如果找不到对应文件,会出现 校验失败,导致下级策略分发失败。

# 17 更新策略

# 17.1 关于更新策略

"更新策略"是管理员操作最为频繁的页面,每次策略更新、 服务器同步、在线认证与授权时都必须通过"更新策略",使天 珣策略系统各组件取得最新策略。

#### 名词解释

"更新策略":是在不影响网络带宽的前提下,根据策略配置的 需求,即时通知天珣策略系统各组件获得最新规则以满足企业策 略变更的需求。

**说明:"更新策略"**不仅包括 WEB 管理控制台(<u>http://localhost:8833</u>) 上由天珣中心服务器主动发送更新策略的指令。"更新策略"也包 括客户端上点击右键"更新策略"。"更新策略"还包括客户端每隔 一个指定的周期重新获取一次策略的系统架构。

# 17.2 更新策略的流程

- 1、客户端向服务器发送客户端报表,服务器确认客户端存在;
- 2、管理员在 web 管理控制台(http://localhost:8833)发送更新策略 指令;

3、天珣中心服务器根据已有客户端报表信息提取 IP 地址列表并以 此表为准向客户端发送更新策略的指令;

4、客户端得到"更新策略"的指令后更新策略。



**注意**:若客户端仍未向服务器发送客户端报表,将无法获知更新策略的指令。

5、客户端若未收到服务器更新策略的指令,用户可以右键点击客

户端"更新策略";

6、"客户端全局参数"-"重新从 Server 上下载策略的时间间隔" 默认值为 24 小时,客户端每 24 小时重新从服务器更新一次规则。

**说明:**策略服务器发送客户端更新策略使用的是 udp 7891 端口,这样比使用 tcp 端口发送更新策略占用网络带宽低。

# 17.3 Server 策略版本页面

### 17.3.1 配置介绍

| Server 建固定保存 建固定保存法 建固定保存法 化   | 使制用ADRUS編輯   |
|--|--|
| 当前管理的策略是外器<br>中心服用者 CasterCorver<br>整理是本 CasterCorver 19, 5, 5, 4<br>图集集本 Internet<br>本块版作者<br>Table Process |  |
| 配置项:   | 说明   |
| 策略版本   | 配置完策略后,可以手工增加策略版本,用以标记该配置。若客户端"关于"项中策略版本和服务器端不同,则客户端未取得新的策略,需手工更新策略。 |
| 增加策略版本   | 每配置新规则时,可点击"增加策略版本"用以标识。   |
| 备份当前策略   | 可以对当前配置的策略进行备份,如果新的策略存在问题,可以用备份的策略快速恢复。                              |
| 策略历史记录   | 即备份的历史策略,点击该按钮可以选择历史策略版本<br>并快速恢复。                                   |
| 本地服务器  | 本地策略服务器受中心策略服务器管理,此处显示了所<br>有本地服务器的相关信息。可以针对单台本地服务器,                 |



|                | 确认策略版本。可以针对单台本地服务器同步策略。 |
|----------------|-------------------------|
| 全部刷新           | 即刷新所有本地服务器的策略版本。        |
| 同步全部 Server 策略 | 即同步所有本地服务器的策略版本。        |

**说明**:本地服务器大多网络独立导致网络时延较大,如果刷新或同步 失败可能由于网络超时导致,建议多此尝试。

## 17.3.2 本地服务器操作简介

- 所有策略均由中心服务器配置和管理,所有报表日志均由中心服务器 web 管理控制台查看。本地服务器只需要获取策略并为客户 端提供服务即可。
- 2、安装完本地服务器后,点击"基本配置-策略服务器"添加本地服务器



3、添加管理网段,该管理网段的第一服务器为本地服务器,第二服



务器为中心服务器。

| 管理网段               |                 |      |
|--------------------|-----------------|------|
| 管理网段名称             | 192. 168. 12    | *    |
| 管理网段描述             |                 |      |
| 管理网段开始IP地址         | 192. 168. 12. 1 | *    |
| 管理网段结束IP地址         | 192.168.12.254  | *    |
| 'rimary Server     | 本地服务器           | •    |
| econdary Server    | CenterServer    | •    |
| 是否使用默认的下载服务器       | ◎否 :● 是         |      |
| 下载服务器地址            |                 |      |
| 亭止客户端服务程序时是否需要验证密码 | ◎ 否 ◎ 是         |      |
| 印载客户端时是否需要验证密码     | ◎否◎是            |      |
| 客户端卸载及停止服务密码       |                 | 显示明文 |

- 4、 配置该管理网段的 IP 组信息(略);
- 5、返回 Server 策略版本页面,将看到本地服务器信息。

| Derverling at A | with class   | EXectores | 1. Willington () |             |               |
|-----------------|--|-----------|------------------|-------------|---------------|
| 当前管理的第          | 685 <b>3</b>   |           |                  |             |               |
| 94883 Cartor    |  |           |                  |             | ANDARS BRATAS |
| Beas filli      | 101107 W. R. R. S. |           |                  | ENVIRON     | 1             |
| C.C.C.          |  | 60.87     | 1000             | ACCRACK CO. | REC-INC.      |

6、点击本地服务器的"刷新"或"同步"按钮将或得本地服务器的 程序版本和策略版本。

**重要:**每配置完策略后,必须将策略同步至本地服务器。若忘记同步规则至本地服务器未取得新策略,导致测试中遇到非预期结果。

#### 17.3.3 配置要点

- 1、配置策略前,选择"Server 策略版本"页面,点击"备份当前策略"。
- 2、 配置完策略后, 选择"Server 策略版本"页面, 点击"增加策略



3、 点击"同步"本地服务器,确保服务器获得最新规则。

# 17.4更新 CC 策略版本页面

#### 17.4.1 配置介绍

- 何时需要更新 CC 策略? 管理员配置了新的安全策略,并要求所 有客户端均需及时同步,则可以及时更新 CC 策略。
- 点击更新 CC 规则后,为什么提示更新完成?提示的是已发出更 新信息,但这并不表示所有客户端已经更新策略。

| Server加速货店 | Record | ERNARIZAN | 更新RADIUS 前编 |          |
|------------|--------|-----------|-------------|----------|
|            |        |           |             | 已发出更新信息! |

#### 名词解释

"CC":即天珣客户端(Client Control)。

#### 17.4.2 配置要点

1、选择更新 CC 策略页面,选择管理网段名称,如下图:

| Server策略版本              | 更新CC策略                            | 更新策略同关策略       | 更新RADIUS策略 |
|-------------------------|-----------------------------------|----------------|------------|
| 即时更新CC策略                | š                                 |                |            |
| 请选择管理问题<br>请为更新CC第酸选择II | - 请选择曾<br>- 请选择曾<br>115 11<br>172 | 整點<br>理阿段-<br> |            |
| 注: +本功能对通过8AT           | 直接服务器的客户属                         | 无效             |            |

2、点击"更新 CC 策略"



| Server策略版本 更             | 新 <u>CC策略</u> 更新 | 新策略网关策略        | 更新RADIUS策略 | ì |
|--------------------------|------------------|----------------|------------|---|
| 即时更新CC策略                 |                  |                |            |   |
| 请选择管理网段<br>请为更新CC策略选择IP组 | 初始管理网段           | <u>帮助</u><br>▼ |            |   |
|                          | 更新CC策略           |                |            |   |
| 注: *本功能对通过NAT连接服         | 务器的客户端无效         |                |            |   |

# 17.5更新策略网关策略页面

### 17.5.1 配置介绍

- 更新"策略网关策略"实际上是通知策略网关代理获取配置的新策略。
- 策略网关代理策略变更必须手工更新才能生效,即每次更改策略 网关策略后必须手动更新策略。
- 需要确保策略网关代理 IP 地址属于已配置的 IP 组,否则无法正常工作。

#### 名词解释

"更新策略网关策略":即通知策略网关获取最新的应用准入策略,因策略网关策略由策略网关代理统一"代理",所以更新的策略实际 是选择策略网关代理的服务器做更新。请参考《用户手册-准入控制-应用准入》。

### 17.5.2 配置要点

选择更新策略网关策略页面,选择策略网关所属的策略服务器,如下图:



| Server策器版本   | 更新CC策略                               | 更新策略同关策略   |   | 更新RADIUS策略 | ) |
|--|--------------------------------------|--|---|------------|---|
| 即时更新策略   | 网关策略                                 |  |   |            |   |
|  |                                      |  | 帮助  |            |   |
| 请选择策略网关代理  | 所属的領職服务器                             | -请选择服务器-   | -   |            |   |
| 请选择策略同关代理  | E                                    | -请选择服务器-   |   |            |   |
|  |                                      | 本地服务器  |   |            |   |
|  |                                      |  |   |            |   |
| . 点击 <b>"更新</b>  | 新策略网关策                               | <b>き略</b> "  |   |            |   |
| . 点击 <b>"更新</b><br>Server策略版本                                      | 新策略网关策                               | を略"<br><u> 更新策略阿关策略</u>  |   | 更新RADIUS策  | ß |
| . 点击 <b>"更新</b><br>Server策略版本                                      | 新策略网关策<br><sub>更新CC策略</sub>          | き略"<br>重新策略网关策略  | 4   | 更新RADIUS策  | 8 |
| . 点击 <b>"更新</b><br>Server策略版本<br>即时更新策略                            | 新策略网关策<br><sup>重新CC策略</sup><br>网关策略  | 更新新略网关策略   | in the second | 更新RADIUS策  | 8 |
| . 点击 <b>"更新</b><br>Server策略版本<br>即时更新策略[                           | 断策略网关策<br><sup>更薪CC策略</sup><br>网关策略  | 迂略"<br><u>更新策略网关策略</u>   | 帮助  | 更新RADIUS策制 | 8 |
| . 点击 <b>"更新</b><br>Server策略版本<br>即时更新策略<br>请选择策略网关代理               | 新策略网关策<br>更新CC策略<br>网关策略<br>所属的策略服务器 | <b>连略"</b><br>更新策略网关策略<br>CenterServer                                     | <u>帮助</u>   | 更新RADIUS策I | 8 |
| . 点击 <b>"更新</b><br>Server策略版本<br>即时更新策略<br>请选择策略网关代理<br>请选择策略网关代理  | 新策略网关策<br>更新CC策略<br>网关策略<br>所属的策略服务器 | <b>连略"</b><br>更新策略网关策略<br>CenterServer<br>全部                               | <u>帮助</u><br>、  | 更新RADIUS策的 | 8 |
| 2. 点击 <b>"更新</b><br>Server策略版本<br>即时更新策略<br>请选择策略网关代理<br>请选择策略网关代理 | 新策略网关策<br>重新CC策略<br>列关策略<br>所属的策略服务器 | <b>更新策略网关策略</b><br><u>更新策略网关策略</u><br>CenterServer<br>全部<br><u>国新策略网关策</u> | <u>耕助</u><br>◆  | 更新RADIUS策制 | 8 |

**注意:**请确保策略网关代理所属策略服务器,如果策略网关代理所在 的管理网段第一服务器不是中心服务器,而是本地服务器。在确保已 经同步本地服务器规则后,更新策略务必选择本地服务器,否则功能 将不正常。



# 17.6更新 RADIUS 策略页面

# 17.6.1 配置介绍

- 更新 "RADIUS 策略" 实际上是通知 radius server 获取配置的 新策略。
- RADIUS 策略变更必须手工更新才能生效,即每次更改准入控制
   策略后必须手动更新策略。
- 需要确保 Radius server IP 地址属于已配置的管理网段,否则 无法正常工作。



### 17.6.2 配置要点

1. 选择"**请选择 RADIUS Server**"下拉列表框,如下图:



# 18. 附录: 单点登录配置手册

# 18.1 天珣单点登录简介

单点登录是指在进行身份认证时,只需输入一次用户身份信息,即可以进行 多次用户身份认证,实现一次登录全网漫游,一次登录全系统漫游。作为新兴的 终端准入控制认证系统,天珣的用户认证是基本要求,安装单点登录功能的天珣 客户端,用户就可只输入一次登录凭证就能实现操作系统及天珣系统的双重身份 认证,也提升了数据的准确性。

天珣单点登录是指安装完特殊的天珣安装包后,在登录操作系统时,只需要 在登录 Windows 系统的时候输入一次登录凭证,天珣客户端就将获取对应的用 户认证信息,后台进行和完成相应的用户认证或者准入控制认证。

# 18.2 单点登录客户端打包

天珣客户端安装包分为普通安装包和单点登录安装包,如果想要具有单点登录功能的话,就必须安装单点登录的安装包,下面就是就其打包的相关选项解释。 启动客户端打包工具,点击"单点登录选项"中的"配置选项",如下图:



| 旨定安装目录 | 1 近小女教相关  |
|--------|---|
| 民装模式   | ● 普通 C 自动 C 静默  |
| 网络准入   | □ 使用802.1X交换机认证 □ 使用EOU认证<br>□ 网络中有道曾53150交换机,否则不建议勾选 |
| 5户端    | ▶ 隐藏客户端图标   |
| 「包模块   | ▶ 文件审计模块 ▶ 移动存储管理模块 ▶ 软件分发模块                          |
| 東登录    | 配置选项 不自用单占容录 默认为"不启用单点                                |
|        | 登录",点击"配置   |
|        | 洗项"则会进入单点   |
|        | 生成客户端安装包  |
|        |   |
|        | 特到各尸婦女装包的仔政日家のおったエットになっ                               |
|        | 将客户端安装包复制到中心服务器的下载目录                                  |
|        |   |

#### 点击"配置选项"进入如下页面

| 单点登录选项         |               |                    | × |
|----------------|---------------|--------------------|---|
| 单点登录;          | ○ 不启用         | •  8月              |   |
| 登录凭证:          | ● 帐号/密码       | C UKEY             |   |
| 网络认证用户类型:      | • 天珣本地用户      | C AD域用户 C 其他LDAP用户 |   |
| Windows本地登录帐号: | ● 安装客户端时的Win  | dows帐号             |   |
|                | C 与网络认证相同的A   | D域帐号               |   |
|                | 〇 以下指定的Window | s帐号                |   |
|                | 指定帐号:         |                    |   |
|                | 帐号类型: 🕝 普;    | 画账号 C 管理员帐号        |   |
| Ti             |               | 取消                 |   |
|                |               |                    |   |

| 配置项:      | <u>说明</u>  |
|-----------|--|
| 单点登录:     | 可选择是否启用单点登录。勾选"不启用",<br>则安装包为普通安装包;勾选"启用",安装<br>包则带有单点登录功能   |
| 登录凭证:     | 选择一种身份认证的方式。<br>帐号/密码 是指在 windows 登录界面上输入帐<br>号密码进行身份认证;<br>UKey 是指在 windows 登录界面上输入智能卡<br>PIN 码进行身份认证 |
| 网络认证用户类型: | 规定天珣客户端以哪一类的用户来进行天珣<br>用户认证。   |



|                     | 天珣本地用户 即天珣自己维护的轻量级的目<br>录服务<br>AD 域用户 即 Active Directory 用户<br>LDAP 用户 即非 AD 域用户的第三方 LDAP 用户  |
|---------------------|---|
| ₩indows 本地登录帐<br>号: | 此帐号是用于规定登录 Windows 系统的帐号。<br>安装客户端时的 Windows 帐号 即安装天珣客<br>户端时的当前 Windows 帐号;<br>与网络认证相同的 AD 域帐号 即以天珣用户认<br>证用户名相同的用户进行 windows 登录,此选<br>项只有当"网络认证用户类型"选择"AD 域用<br>户"时才可选;<br>以下指定的 Windows 帐号 指定一个登录<br>windows 系统的帐号 |
| 指定帐号                | 当"Windows 本地帐号"选择为"以下指定的<br>Windows 帐号时",此项才变为可编辑,可指<br>定登录的帐号名同帐号类型  |

选择完相关选项后,点击"确定"就跳转到打包工具的初始界面,生成客户端安装包,此安装包就是具有天珣单点登录功能的安装包了。

# 18.3 天珣单点登录的两种登录方式

天珣单点登录按照登录凭证可分为帐号/密码单点登录和 UKEY 单点登录, 其主要区别在于登录方式的不同,下面就这两种登录方式做详细介绍。

#### 18.3.1 帐号/密码单点登录

帐号/密码单点登录是指在 windows 登录界面上,输入用户名及密码并选择 所需登录的域从而实现两次用户身份认证的登录方式(两次用户身份认证是指 Windows 身份认证及天珣用户认证)。帐号/密码登录支持的用户类型包括天珣本 地用户、AD 域用户、LDAP 用户。详细配置示例如下,具体注意事项如下:

注意:

- "基本配置"—"用户组"—"目录服务",这里可以新增一个目录服务, 新增加的目录服务名称必须与目录服务路径的第一个 dc 值一致;如目录服务的路径为 dc=sunshine, dc=com,则目录服务名称就为 sunshine;
- 如果客户端没有启用用户认证时,选择"用户名/密码登录"登录方式登录
   时,无法成功登录
- 如果终端的用户认证是网络准入下的用户认证,则只有当网络准入通过后, 才能成功登录系统



以如下打包选项为例: 登录凭证:帐号/密码 网络认证用户类型:天珣本地用户 Windows 本地登录帐号:安装客户端时的 Windows 帐号

(1) 打包账户/密码登录方式的客户端,见下图,具体解释详见 18.2

| 单点登录;          | ○ 不启用                       | ● 启用      |            |
|----------------|-----------------------------|-----------|------------|
| 登录凭证:          | € 帐号/密码                     | C UKEY    |            |
| 网络认证用户类型:      | ☞ 天珣本地用户                    | C AD域用户   | C 其他LDAP用户 |
| Windows本地登录帐号; | <ul> <li>安装客户端时的</li> </ul> | Windows帐号 |            |
|                | C 与网络认证相同的                  | 的AD域帐号    |            |
|                | ○ 以下指定的Wind                 | lows帐号    |            |
|                | 指定帐号:                       |           |            |
|                | 帐号类型: 6                     | 普通帐号 C 管  | 理员帐号       |

(2) 终端安装步骤(1)打包出来的客户端,重启终端,windows登录界面变为如下页面

| 欢迎使用 ♥indows   |                   |      |  |
|----------------|-------------------|------|--|
| Balatenukseesa | 开始<br>为于维护您的计算机的S | 2全性。 |  |

按 ctrl+Alt+delete 跳转到登录界面, vista 以下版本同 vista 以上版本登录界面分别如下:





| 天狗单点登录  |         |      |  |
|---------|---------|------|--|
| 客户端服务已启 | 动,请输入用户 | 中名密码 |  |
| 用户名:    |         |      |  |
|         |         |      |  |
| 密码:     |         |      |  |
|         |         |      |  |
| 域:      |         |      |  |
|         |         |      |  |
| 确定      | 取消      | 关机   |  |
|         |         |      |  |
|         |         |      |  |



Vista 及以上版本可能初始登录框不是上图,这是点击"切换用户"就 ok 了。 见到上图后,就说明你客户端的配置已成功完成了,先恭喜你了;下面再跟着我 转到服务器端进行相关信息配置了。

(3)首先,进入天珣 Web 控制台(Web 页面),在 Web 控制台上为客户端启用用 户认证,非网络准入下的用户认证或者是网络准入下的用户认证; 非网络准入下的用户认证

**"基本配置"一"IP 组" "是否启用用户认证"**勾选为启用,并选择你所有 启用的目录服务



|                    | 100                    | 10.001.000.1 | 10 101 110 298 | 1 X            |  |
|--------------------|------------------------|--------------|----------------|----------------|--|
| NHR1851            |                        | 207328       |                | 111 121<br>231 |  |
| 16814              | TARINHA                | -            |                |                |  |
| IT BERNER<br>WEINE | ESIOR                  |              |                |                |  |
| 是其由用用户记录           | 07.68                  |              |                |                |  |
| sécretes           | €an<br>R≭#n≓<br>Rombos |              |                |                |  |
| N.F. IF, NORMALE   | N TAR<br>Cita          |              |                |                |  |
| Although .         | 0.131<br>#7.08         |              |                |                |  |

#### 网络准入下的用户认证

"准入控制"—"网络准入"—"radius server",点开一个 radius server 配置项,勾选用户认证,并且选择要启用的目录服务

| RADIUS Server                                       | 利用wwenthisting 的现在分词分子的问题 | RUERACRERA | VLANER | 豊富19歳 |
|---|---------------------------|------------|--------|-------|
| RADIUS Server                                       |                           |            |        |       |
| BEDS Server B/B                                     |                           |            |        |       |
| 16d   | 88                        | -          |        |       |
|   |                           | -          |        |       |
| 17地址  | 18.201.86.8               | 12         |        |       |
| USING   |                           |            |        |       |
| FR64D.AD  | in endings to             |            |        |       |
|   | C BROTTRAN IN             |            |        |       |
|   | 0.84                      |            |        |       |
| 教育内容  | © (NET PROT               |            |        |       |
|   | * RPUR                    |            |        |       |
|   | 一 用整有的利户认证                |            |        |       |
| 进程和利用和服用服件  | RateArt                   |            |        |       |
|   | Winative                  |            |        |       |
| 第1月1日 日本 18日本 19日本 19日本 19日本 19日本 19日本 19日本 19日本 19 | # 不前用                     |            |        |       |
|   | 0.0                       |            |        |       |
|   | 0.00                      |            |        |       |

页面配置完成后,在 web 控制台上更新 CC 策略(非网络准入)或者更新 radius 策略(网络准入)。

至此页面上的配置也就基本完成了,现在我们再回到客户端的 windows 登录界面,之前已经有 windows 登录界面的截图了,在用户名、密码输入框输入正确的用户名同密码,并且选择该用户名所对应的域名称,点击"确定"。

成功登录系统后,右键天珣客户端点击"用户登录控制"发现天珣自带的用户认证也已成功完成了。

#### 18.3.2 UKey 单点登录

Ukey 单点登录是指在 windows 登录界面上, 输入 Ukey 的 PIN 码从而实现两 次用户身份认证的登录方式(两次用户身份认证是指 Windows 身份认证及天 珣用户认证)。UKey 单点登录支持天珣自带的轻量级 CA 和第三方 CA 机构。详细配置示例如下, 先查看如下注意事项



#### 注意:

- ◆ 用于 UKey 单点登录的 UKey 必须具有支持智能卡登录操作系统的功能,如: epass 3000、epass 2000FT (epass 2000 FT 不支持 Windows7 系统)
- 目前天珣系统自带的 CA 只支持将证书颁发到飞天诚信的 UKey,请确认你 UKey 的牌子及型号
- 如果天珣客户端跟天珣服务器未连通时,则会采用之前的缓存登录,但必 须有一次成功登录缓存登录功能才会生效
- "基本配置"—"用户组"—"目录服务",这里可以新增一个目录服务, 新增加的目录服务名称必须与目录服务路径的第一个 dc 值一致;如目录 服务的路径为 dc=sunshine, dc=com,则目录服务名称就为 sunshine;
- 如果客户端没有启用用户认证时,选择"用户名/密码登录"登录方式登录时,无法成功登录
- 如果终端的用户认证是网络准入下的用户认证,则只有当网络准入通过
   后,才能成功登录系统

以如下打包选项为例: 登录凭证:UKey 网络认证用户类型:AD域用户 Windows 本地登录帐号:与网络认证相同的 AD 域帐号

(1) 打包 Ukey 登录方式的客户端,见下图,具体解释详见 18.2

| ○ 帐号/密码     | C LIVEN   |   |
|-------------|---|---|
|             | V UKEY  |   |
| ○ 天珣本地用户    | ● AD域用户   | C 其他LDAP用户  |
| ○ 安装客户端时的   | Windows帐号   |   |
| • 与网络认证相同   | 的AD域帐号  |   |
| ○ 以下指定的Wind | dows帐号  |   |
| 指定帐号:       |   |   |
| 帐号类型: で     | 普通帐号 C 管  | 理员帐号  |
|             | <ul> <li>○ 天珣本地用户</li> <li>○ 安装客户端时的</li> <li>○ 与网络认证相同</li> <li>○ 以下指定的Winc</li> <li>指定帐号:</li> <li>「</li> <li>帐号类型:</li> <li>○</li> </ul> | <ul> <li>              ・ 天珣本地用户             ・ AD域用户      </li> <li>             ・ 安装客户端时的Windows帐号         </li> <li>             ・ 与网络认证相同的AD域帐号         </li> <li>             ・ 以下指定的Windows帐号             指定帐号:<br/>・ 転号类型:             ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・</li></ul> |

(2) 终端安装 UKey 驱动,并且终端加入域,务必记住要安装 UKey 驱动,未安装该驱动就无法采用 UKey 登录系统了

(3) 终端安装步骤(1)打包出来的客户端,重启终端,windows 登录界面变为如下页面





按 ctrl+Alt+delete 跳转到登录界面, vista 以下版本同 vista 以上版本登录界面分别如下:



Vista 及以上版本可能初始登录框不是上图,这是点击"切换用户"就 ok 了。 见到上图后,就说明你客户端的配置已成功完成了,先恭喜你了;下面再跟着我 转到服务器端进行相关信息配置了。

以 windowsCA 为例, windowsCA 安装及证书生成详见 18.4

- (3) 首先,进入天珣 Web 控制台(即 Web 页面),进入<u>"认证管理→第三方</u> <u>CA 机构"</u>添加一个第三方 CA 根证书;
- (4) 根证书添加完成后,再去到"认证管理→身份认证",在"用户及证书信息管理"页面上导入 AD 域用户,详见 <u>14.3.2</u>;
- (5) 将导入的第三方用户同 UKey 里面的证书相关联。只需要在"用户及证书 信息管理"页面上,点击你需要关联的那个用户后,在"证书用户名" 里填写 UKey 里面的证书用户名;详见 14.3.2;
- (6) 配置完上面这些之后,进入最后一个配置环节:为客户端启用用户认证。 启用方法同帐号/密码单点登录的第(3)步配置;

配置完成后,在 web 控制台上更新 CC 策略(非网络准入)或者更新 radius 策略(网络准入)。

至此页面上的配置也就基本完成了,现在我们再回到客户端的 windows 登录界面,之前已经有 windows 登录界面的截图了,将 UKey 接入安装了单点登录客户端的终端后,在 PIN 码对应的输入框输入正确 PIN 码,点击"确定"即可登录了。至此,UKey 单点登录功能也算大功告成了。

成功登录系统后,右键天珣客户端点击"用户登录控制"发现天珣自带的用户 认证也已成功完成了。

# 18.4 配置利用智能卡进行 windows 身份验证

#### 准备工作:

- 1、搭建域环境
- 2、安装 IIS, 并将"Active Server Pages" 服务设置为"允许"



3、客户端加入域以及相关 USBKey 驱动安装


4、 将 IE 的安装设置 设置为"中低",并启用任何"ActiveX 控制和插件",然 后将证书服务器地址添加到"可信任站点中"





| 703 (A) |
|---------|
|         |
| 19.92   |
|         |
|         |

- 一、安装证书服务器
- 打开"windows组件安装",选择"证书服务"

| adama MIC           |                  |                              |
|---------------------|------------------|------------------------------|
| 可以添加成量時にメリン         | lees 的组件。        |                              |
| 要添加或租税基个组/          | *,读单击旁边的发送框。东    | 色框表示只会安美证则内的                 |
| 一部分,要查看這件           | 5容,请单击"详细信息"。    |                              |
| 相件(0)-              | S                |                              |
| 図 可应用程序服务           |                  | 34.4.80 <u>m</u>             |
| □ 通话程存储             |                  | 6.1.83                       |
| 四日 经利用金             |                  | 1.4.83                       |
| □                   |                  | 0.0 ND                       |
| 1.1.7.320688-0-3846 |                  | 0.9 HB                       |
| 描述 安美证书             | 最优机构 (CA)以便最黄语书用 | 于公朝安全程序。                     |
| 所要制度交流              | 4.9.93           | Sector Contractor Contractor |
| 可用組織空间              | 15805.2 MD       | 974B0LB (Q)                  |
|                     |                  |                              |
|                     |                  |                              |

选择"企业根 CA"

注明:要颁发智能卡登录证书,必须选择"企业根 CA"才可以使用, 企业根 CA 和独立根 CA 都是证书颁发体系中最受信任的证书颁发机构,可以独立 的颁发证书。企业根 CA 需要 Active Directory 支持,而独立根 CA 不需要,从 属级的 CA 由于只能从另一证书颁发机构获取证书,所以一般不被选择。而创立 根主要用于外部网的 CA,在安装后不能增加证书模板,不能颁发智能卡证书, 所以我们这里不选择独立 CA ľ



| 44+++ 组件内导<br>CA 类型<br>选择您想设置的 C  | · 京型.        |           |     | ß  |
|---|--------------|-----------|-----|----|
| ○ 法当時 CA(E) ○ 法当時 CA(E) ○ 法当時 CA(E) ○ 法立時 CA(E) ○ 法立規範 CA(E) ○ 法立規範 CA(E) |              |           |     |    |
| CA 吴星的描述<br>企业中最美信任R  | ) (4. 应该在安美英 | 地 CA 之前安装 | £   |    |
| 「「用自定文设置生   | 或连続对称 CA 迁非  | œ         |     |    |
|   | (F-40)       | F         | R/R | 相助 |

输入证书的识别名称,这里我们输入"hetech"

| CA 说别信息<br>输入识别语 CA 的的 | äē.                 | C     |
|------------------------|---------------------|-------|
| 此 CA 的公用名称 (C):        |                     |       |
| hetech                 |                     |       |
| 可分期名称后缀(亚):            |                     |       |
| DC=hctech, DC=con      |                     | 1     |
|                        |                     |       |
| 可分耕名称的预览(1):           |                     |       |
| CH=hstech, DC=hstech,  | DC≠com              |       |
|                        |                     |       |
| 有效期限(2):               | 截止日期                |       |
| 5  4 1                 | 2013-5-9 14:44      |       |
|                        |                     |       |
|                        | characteria and the | 87.04 |
|                        | (上一歩(3) 下一歩(0)) 取用  | 帮助    |

选择证书数据库和日志的安装路径,我们设置为默认

| 此"印刷"集團""[1]:                 |  |
|-------------------------------|--|
| NAMINONSAnystem32ACertLor     | <b>潤荒 (Q)</b>  |
| 正书取据库日志 Q):                   | The second s |
| C:\WINDOWS\system32\CertLog   | <b>浏览(生)</b>   |
| 裕配費信息存線在共享文件夹中で)<br>共享文件夹(U): | <b>潮流 (1</b> ) (1)   |
|                               |  |
| Image00003.jpg                |  |

安装证书服务需要重启 IIS 服务,我们这里选择"是"



#### 安装证书服务



安装证书完毕后,进入第二个阶段,

#### 下载证书

打开 IE,访问证书服务器的地址<u>http://证书服务器的 IP 地址/certsrv</u>, 下载一个证书:

| E.QI Matty //Londhoot/environTafaalt. say                                | 土 🌆 林龍 🕷                            |
|--|-------------------------------------|
| Gerrandt 2488 - Interio  | 11                                  |
| 「遊   |                                     |
| t用此网站为坦的 Reb. 浏览器,电子邮件客户端或其他程序申请一个证<br>eb. 通信的人确认您的身份,签署并加密邮件,并且,根据您申请的证 | 1节,通过使用证书,但可以和通过<br>11的类型,执行其故安全任务。 |
| 出可以使用此同站下载证书重发机构(CA)证书。证书摄,或证书易销<br>5。                                   | 列表(CRL)。或查看挂起的申请的状                  |
| 关证书服务的评调信息,请参供证书服务文档。  |                                     |
| ○ 一个任务:<br>申请一个位书<br>查看推起的证书申请的状态<br>学家一个 CA 证书, 证书随后 CEL                |                                     |
|  |                                     |

选择"下载 CA 证书"



| Biersteft @ 888 - Biersteft lafternet Ragberte               | RIS E                                    |
|--|--|
| 文件(1) 編集(1) 重要(1) 作用(1) 工具(1) 特許(1)                          |  |
| QAR - O - O A C PRE ORR C - O - O T                          |  |
| 戦戦 ② 💼 http://localbent/carture/carturals.aug                | · () () () () () () () () () () () () () |
|  |  |
|  |  |
| 下载 CA 証书, 証书链ي CRL   |  |
| 原体任何这个位书领受招助领导的过去。 安装在 (4) 位书馆。                              |  |
| NED TRACE I THE COMPLETE COMPLETE OF THE PARTY OF THE PARTY. |  |
| 要下载一个 CA 证书。证书继续 CRL,选择证书和编码方法。                              |  |
| CA 证书:   |  |
| Image00007.[pg]  |  |
|  |  |
|  |  |
| 编码方法。  |  |
| of turn  |  |
| C Base 64  |  |
| 下款 CA 证书   |  |
| 王欽 CA 证书通  |  |
| 下载最快的基(BL  |  |
| 之职總統的理論。(四   | 10                                       |
| 0  | No 218 Cotranat                          |

# 选择保存路径:

| FF下载 - 安全   | 2.等合   |   |            |
|---|--|---|------------|
| 您想打开或保存   | 手此文件吗?   |   |            |
| 名<br>共<br>发送  | 称: certnew.cer<br>型: 安全证书, 1.10 IB<br>者: localhost                                       |   |            |
|   | 打开②  | 存⑤ [                                      |            |
| (1) 米息)   | Internet 的文件可能对您有所<br>IOPDit首机,如果你不信任何   | 所帮助,但此文件类型。<br>【来源:法不要打开进》                | IJ         |
| ● 精選載   | 路的打算机。如果这个语世界<br>件。 <u>有何风险?</u>   | 476 A B A B A B A B A B A B A B A B A B A | <b>*</b> : |
| 行为  |  |   | 2          |
|   |  |   |            |
| 保存在 (1)   | da (   | 2002                                      | · .        |
|   | ● 桌面<br> 我的文档<br>  我的电脑<br>  网上邻居  | 2 O Å D                                   |            |
| 保存在 Q)<br>保存在 Q)<br>()<br>()<br>()<br>()<br>()<br>()<br>()<br>( | <ul> <li>● 桌面</li> <li>● 我的文档</li> <li>● 我的文档</li> <li>● 阿上邻居</li> <li>● 阿上邻居</li> </ul> | 2 O Å 2                                   | [ ● ●      |

下载完毕后, 接下来需要导入到机器中

# 导入根证书



打开 IE 属性,选择"内容一》证书"

| net AllE                 | _      | 0               |            |
|--------------------------|--------|-----------------|------------|
| , 安全 隐私 内容               | 连接     | 程序 高            | z          |
| )级审查                     |        |                 |            |
| 分级系统可帮助您控制 内容。           | 则在设计算用 | L上看到的 In        | ternet     |
|                          | 启用 (L) |                 | 30         |
|                          |        |                 |            |
| 使用证书可正确标识》               | 8自己。证书 | SERVER AL ACTOR | -00010.jpg |
| 身份。                      |        | -               |            |
| 诸除 SSL 状态 (5)            | 证书(C)  | 发行商             | a) [       |
|                          |        |                 |            |
| ~A18.8                   |        |                 | 11         |
|                          | 机前的条目并 | 梅 自动完成          | z oo       |
| 10 村台的项目推荐始送。            |        | <u></u>         |            |
|                          |        |                 |            |
| Microsoft 配置文件単<br>小人信息。 | 力理能存储总 | 的配置文件           | # (B)      |
|                          |        |                 |            |



| 制度18 |     | 截止日期 | 好记的名称 | I |
|------|-----|------|-------|---|
|      |     |      |       |   |
|      |     |      |       |   |
|      | /// |      |       |   |

进入证书导入向导,进入"下一步"







选择证书存放的方式,这里我们选择默认

|                |                                   | 44-100 |
|----------------|-----------------------------------|--------|
| Tindows 可以自动选择 | 业书存储; 或者您可以为证书指定一个<br>自动表提证书本律 on | VE-    |
| () 將所有的证书前     | 日本の近時近1797日(型)<br>入下刻存储(P)        |        |
| 证书存储:          |                                   |        |
| 不不             |                                   | 浏览(2)  |
|                |                                   |        |
|                |                                   |        |
|                | Image00014.jpg                    |        |



| 证书导入内导 |                       |                             | ×         |
|--------|-----------------------|-----------------------------|-----------|
|        | 正在完成证书                | 5导入向导                       |           |
|        | 悠已成功地完成证              | 书导入向导。                      |           |
|        | 悠已指定下列设置              | Ť                           |           |
|        | 用户达定的加卡的<br>内容<br>文件久 | イ人<br>近书<br>C:\Nermants and | Settines) |
|        | 2013                  |                             |           |
|        |                       |                             |           |
|        | •                     |                             | <u>.</u>  |
|        |                       |                             |           |
|        | <u>&lt;</u> ±         | 一步® 完成                      | 取消        |



导入完成后,我们可以在"中级证书颁发机构"和"受信任的根证书颁 发机构"中看到刚导入的证书信息

| STATES IN CONTRACTOR   |  |  |  |              |
|--|--|--|--|--------------|
| 期目的(29): (所有>  |  |  |  | 1            |
| 个人   其他人 中级证书颁发机构 受信任的格  | 证书顶发机构   | 2 受信任的   | 发行者  | i.           |
| e00032.jpg   |  | - 1 - 2 - 1 - 2 - 1 - 2 - 1 - 2 - 1 - 2 - 1 - 2 - 1 - 2 - 2  | 0012.01  |              |
| - 印发给  | 截止日期   | 好记的名   | <u>ل</u>   |              |
| Ehctech hctech   | 2013-5-9   | (Æ)  | 1  |              |
| Microsoft Wind Microsoft Boot A  | 2002-1   | 〈无〉  |  |              |
| Boot Agency Boot Agency  | 2040-1-1   | (元)  |  |              |
| VeriSign Class Class 1 Public P  | 2008-5-13  | 《无》  |  |              |
| VeriSign Class Class 2 Public P  | 2004-1-7   | 〈九〉  |  |              |
| www.verisign.c., Class 3 Fublic F  | 2004-1-8   | 0022   |  |              |
| <br>导入( <u>(</u> )   _导出(( <u>)</u> )   _删除(( <u>6</u> )   |  |  | 高级(  | φ            |
| 证 #iphfe期目 ph  |  |  |  |              |
| 1409124914199  |  |  |  |              |
| V01H 2   |  |  | -  | en:          |
|  |  |  | 重有化  | 2            |
|  |  |  |  |              |
|  |  |  |  |              |
|  |  |  | 美田   | (C)          |
|  |  |  | 关闭   | (Ç)          |
| 5  |  |  | 关闭   | ( <u>c</u> ) |
| S Correction   |  |  | 关闭   | (c)          |
| 購目的 00: (所有>   |  | -  | 关闭   | ( <u>c</u> ) |
| 5<br>期目的 900: (所有><br>下人   其他人   中颌证书喷发机构 受信任的根  | 证书硕发机科   | 夏信任的   | 关闭   | ( <u>c</u> ) |
| 5<br>期目的 92): (所有)><br>下人   其他人   中颌证书喷发机构 受信任的短<br>「疲发给   强发者   | □王书硕发机料<br>【業止日期】  | ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●  | ( 美田<br>3)发行者  <br>称   | •            |
| 5<br>期目的 QD: (所有)<br>下人 其他人   中颌证书喷发机构 爱信任的概<br>[ 疲发给   顽发者<br>[ ] GTE CyberTrust G  | □ #4個发机和<br>■ 截止日期<br>2018-8-14  | ·<br>天信任的<br>GTE Cyber   | ( 关闭<br>3发行者)<br>称<br>rTra   | ()<br>•      |
| 5<br>期目的 QD: 《所有》<br>下人 】其他人   中颌证书领发机构 爱信任的相<br>  | □ 书研发机和<br>■ 截止日期<br>2018-8-14<br>2004-4-4   | 受信任的<br>好记的名:<br>GTE Cybes<br>GTE Cybes  | (关闭<br>的发行者)<br>称<br>rTru  | •            |
| 5<br>期目的 QD: (所有)<br>下人   其他人   中颌证书领发机构 受信任的相<br>领发给   颁发者<br>回 GTE CyberTrust GTE CyberTrust G<br>回 GTE CyberTrust GTE CyberTrust Root<br>回 GTE CyberTrust GTE CyberTrust Root   | 证书领发机和<br><b>截止日期</b><br>2018-8-14<br>2004-4-4<br>2006-2-24  | 受信任的<br>好记的名J<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes  | 关闭<br>助发行者<br>称<br>rTru.<br>rTru.<br>rTru.   |              |
| 5<br>期目的 QD: (所有)<br>下人   其他人   中額証书機发机构 受信任的相<br>微发给 - 一 微发着<br>回 GTE CyberTrust GTE CyberTrust G<br>回 GTE CyberTrust GTE CyberTrust Soot<br>回 GTE CyberTrust GTE CyberTrust Soot   | 证书领发机和<br>截止日期<br>2018-8-14<br>2004-4-4<br>2006-2-24<br>2013-5-9   | 受信任的<br>好记的名词<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes  | 关闭<br>b发行者<br>称<br>rTru.<br>rTru.  |              |
| 5<br>期目的 00: (所有)<br>下人   其他人   中初证书领发机构 爱信任的纲<br>须发给   须发者<br>回 GTE CyberTrust GTE CyberTrust G<br>回 GTE CyberTrust GTE CyberTrust Soot<br>回 GTE CyberTrust GTE CyberTrust Soot   | 世书领发机和<br>2018-8-14<br>2004-4-4<br>2006-2-24<br>2013-5-7<br>2013-5-7   | 受信任的<br>好记的名词<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes   | 文明<br>文字書  |              |
| 5<br>期目的 00: (所有)<br>下人   其他人   中初证书领发机构 受信任的相<br>资发给 / 资发者<br>回 GTE CyberTrust GTE CyberTrust G<br>回 GTE CyberTrust GTE CyberTrust Root<br>回 GTE CyberTrust GTE CyberTrust Root<br>I CyberTrust GTE CyberTrust GTE CyberTrust Root<br>I CyberTrust GTE CyberTrust  | 世书颁发机制<br>就止日期<br>2018-8-14<br>2004-4-4<br>2004-4-4<br>2003-5-7<br>2013-5-7<br>2013-5-9<br>2019-8-26   | 受信任的<br>好记的名3<br>GTE Cybes<br>GTE | ( 美田<br>)安行春<br>「Tru.<br>「Tru.<br>「Tru.<br>「Tru.   | •            |
| 5<br>期目的 00: 所有><br>下人   其他人   中初证书领发机构 受信任的相<br>资发给 / 资发者<br>回 GTE CyberTrust GTE CyberTrust G<br>回 GTE CyberTrust GTE CyberTrust Root<br>回 GTE CyberTrust GTE CyberTrust Root<br>I ColeCh / Matech<br>Detech / hetech<br>Detech / hetech / hetech<br>Detech / hetech / hetech<br>Detech / hetech / hetech   | 日本語彙机構<br>一種止日期<br>2018-6-14<br>2004-4-4<br>2006-2-24<br>2013-5-9<br>2013-5-9<br>2019-6-26<br>2019-6-26  | 受信任的<br>好记的名類<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>(元)<br>(元)<br>(元)<br>ValiCert<br>ValiCert   | ( 关闭<br>)发行者<br>「Tru.<br>rTru.<br>rTru.<br>cla.<br>Cla.  |              |
| 期目的 00: (所有)<br>下人   其他人   中颌证书顽发机构 受信任的感<br>適定差 CyberTrust GTE CyberTrust G<br>GTE CyberTrust GTE CyberTrust Root<br>GTE CyberTrust GTE CyberTrust Root<br>GTE CyberTrust GTE CyberTrust Root<br><b>Rotech</b><br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>Photech<br>P | <ul> <li>1日期</li> <li>2018-8-14</li> <li>2008-8-14</li> <li>2008-2-24</li> <li>2013-5-7</li> <li>2013-5-7</li> <li>2013-5-7</li> <li>2013-5-9</li> <li>2019-6-26</li> <li>2019-6-26</li> <li>2019-6-26</li> <li>2019-6-26</li> </ul> |  | 关闭<br>数行者<br>称<br>rTru<br>rTru<br>rTru<br>cla.<br>cla.<br>cla.   |              |
| 5<br>期目的 QD: (所有)<br>下人   其地人   中颌证书领发机构 爱信任的纲<br>一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一  | 近年3項发机和<br>2018-8-14<br>2004-4-4<br>2006-2-24<br>2013-5-7<br>2013-5-7<br>2013-5-9<br>2019-6-26<br>2019-6-28<br>2019-6-28   | 受信任的<br>好记的名が<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>(元)<br>(元)<br>(元)<br>ValiCert<br>ValiCert<br>ValiCert  | 美田<br>動数行著<br>の<br>な<br>で<br>Tru<br>で<br>Tru<br>で<br>Tru<br>で<br>し<br>。<br>の<br>で<br>こ<br>し<br>。<br>の<br>の<br>で<br>し<br>、<br>の<br>で<br>し<br>、<br>の<br>で<br>し<br>、<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の   |              |
| 期目的 QD: (所有)<br>所人   其他人   中切証书優发机构 爱信任的期<br>一切差 CyberTrust GTE CyberTrust G<br>回 GTE CyberTrust GTE CyberTrust Soot<br>回 GTE CyberTrust GTE CyberTrust Soot<br>GTE CyberTrust GTE CyberTrust Soot<br>回 GTE CyberTrust GTE CyberTrust Soot<br>回 GTE CyberTrust GTE CyberTrust Soot<br>回 GTE CyberTrust GTE CyberTrust Soot<br>I GTE CyberTrust   | 日本語文机構<br>2018-8-14<br>2004-4-4<br>2004-4-4<br>2005-2-24<br>2013-5-9<br>2013-5-9<br>2019-6-26<br>2019-6-26<br>2019-6-26  | 受信任的   | 关闭<br>数行者<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre.<br>erre |              |
| 5<br>期目的 00: (所有)<br>下人   其他人   中颌证书感发机构 受信任的想<br>一切五 CyberTrust GTE CyberTrust G<br>一 GTE CyberTrust GTE CyberTrust Root<br>一 Matech Actech<br>一 Matech Actech<br>— Matech Actech Actech<br>— Matech Actech<br>— Matech Actech<br>— Matech Actech Actech<br>— Matech Actech Actech<br>— Matech Actech<br>— Matech Actech Actech Actech<br>— Ma  | 世界優发初料<br>2018-8-14<br>2004-4-4<br>2004-4-4<br>2004-5-24<br>2013-5-7<br>2013-5-9<br>2019-6-26<br>2019-6-28<br>2019-6-28  | 受信任的<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>GTE Cybes<br>(元)<br>(元)<br>(元)<br>ValiCert<br>ValiCert<br>ValiCert  | 关闭<br>数行者<br>%<br>Tru.<br>rTru.<br>cla.<br>cla.<br>cla.<br>cla.<br>cla.<br>cla.<br>cla.<br>cla   |              |

添加证书模板

打开管理工具,选择"证书颁发机构"



|   | 2 (H)  |   |  |
|---|--|---|--|
| <ul> <li>○ 正中研究所用はは</li> <li>○ Lettel</li> <li>○ 計算的に</li> <li>○ 指数的に</li> <li>○ 指数的に</li> <li>○ 注意の中語</li> <li>○ 注意の中語</li> <li>○ 注意の</li> </ul> | 支統<br>日学电子部件复制<br>国地艺和局负伯祉证<br>国地艺和局<br>通地艺和局<br>国地艺和局<br>国内<br>国内<br>国内<br>国内<br>国内<br>国内<br>国内<br>国内<br>国内<br>国内<br>国内<br>国内<br>国内 | 2011日的<br>日子服装成电子邮件复制<br>客户端能证 服务器能证 智能十里荣<br>次年初期抗复<br>加密文件系统<br>客户端能证 服务器能证<br>家户端能证 服务器能证<br>加密文件系统 安土电子邮件,客户<br>(所有)<br>Niccosoft 保任列表量名、加密文件 |  |



| (二年)(四年)(11)(二十年)   | ŚR  | - Hall Ruh   |
|---|---|--|
| <ul> <li>□ 正书(初安和构(市地))</li> <li>□ Arteck</li> <li>□ 新文的定书</li> <li>□ 形式的字目</li> <li>□ 形式的字目</li> <li>□ 予約(中)目</li> <li>□ 予</li></ul> | 名称<br>日季电子都件复制<br>同时来电子都件复制<br>同时来世代型<br>同时来世代型<br>同时来世纪的<br>同时,世纪和<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪》<br>一世纪<br>一世纪<br>一世纪<br>一世纪<br>一世纪<br>一世纪<br>一世纪<br>一世纪 | 型種種的<br>目子服条电子部件复制<br>客戶機動证、服务器制证、智能卡整条<br>文件創種恢复<br>加密文件系统<br>整戶機動证<br>服务器制证<br>服务器制证<br>加密文件系统、安全电子邮件、零户<br>(所有)<br>Biocrossft 信任利费妥名、加密文件<br>ImageD0017.jpg |
|   |   |  |

选择要启用的证书模板:智能卡用户、智能卡登录、注册代理、注册代 理(计算机),然后"确定"



出

| 名称              | 预期目的               |   |
|-----------------|--------------------|---|
| 國信任列表签名         | ■icrosoft 信任列表签名   |   |
| 同只是 Ixchange 签名 | 安全电子邮件             |   |
| 只是用户签名          | 安全电子邮件,客户端验证       |   |
| 回密钥恢复代理         | 密钥族复代理             |   |
| 了工作站身份验证        | 客户藏验证              |   |
| 122 智能卡用户       | 安全电子邮件,客户端验证,智能卡置录 |   |
| 電智能卡登来          | 客户端验证,智能卡登录        |   |
| 國注册代理           | 证书申请代理             |   |
| 國注册代理(計算机)      | 证书申请代理             |   |
| 2· 经过载证的会估      | 客戶讓验证              |   |
| 国路由器(脱机申请)      | 客户端验证              | 2 |

### 申请注册代理

打开 mmc, 然后添加"证书"管理单元

|         | 清键入程月<br>称,Windo | F、 文件夹、<br>vs | 文档或 Int<br>7开它。 | ernet 资源的 | 的名     |
|---------|------------------|---------------|-----------------|-----------|--------|
| 打开 (2): | and              |               |                 |           | •      |
|         |                  | 确定            |                 | 浏覧 Q      | 0      |
| n 经和合   | 1                |               |                 |           | No. 10 |
| 文件(E)   | 操作(3)            | 查看创           | 收藏买(0)          | 窗口 (g)    | 帮助创    |
| 新建 08   | )                |               | Ctr1+B          |           |        |

 1
 2件(生) 操作(金) 查看(Y) 收藏天(型) 個口(Y) 帮助(D)

 新建(B)
 Ctrl+B

 打开(型)
 Ctrl+B

 (保存(S)
 Ctrl+B

 第方方(金)
 Ctrl+B

 添加/曲除管理单元(B)
 Ctrl+B

 違項(C)
 ...

 主控制台1.msc
 ...

 2 C: \WINDOWS\system32\dss.msc
 ...

 3 C: \WINDOWS\...\compagnt.msc
 ...

 1 控制台1.msc
 ...

 2 C: \WINDOWS\...\compagnt.msc
 ...

 1 C: \WINDOWS\...\cortsrv.msc
 ...

 1 2出(Q)
 ...



|  |   | 节点   | 1   | 面 |
|--|---|--|---|---|
| 描述   |   |  |   |   |
| 添加 (1)   | H92(2)  | 关于(1)  |   |   |
| 添加(Q)<br>1   | <u>田時(g)</u>  | 关于(1)  |   | ? |
| 添加 (Q)<br>1.快び管理单元<br>用的独立管理单<br>管理单元  | ₩₽2:(2) 」   | <u>关于(g)</u><br>供应商  |   | ? |
| 添加 (Q)<br>中独 2 合 理 单 元<br>用的 独立管理 单<br>管理 单 元<br>重求引服务   | 田戸(Q)  <br> <br> <br> 近:  | 关于(g)<br>供应槽<br>Microsoft  | . Corpors   | ? |
| 添加 (Q)<br>中 (A)  | 田序(2)  <br> <br> 元:   | 关于(g)<br>供应商<br>Microsoft<br>Microsoft   | Corpors   | ? |
| 添加 (Q)   | 田序(2) (   | <del>关于(g)</del><br>供应商<br>Microsoft<br>Microsoft<br>Microsoft   | Corpors<br>Corpors<br>Corpors   | ? |
| 添加 (Q)<br>中 文 管 理 单 元<br>雷 索 引服务<br>) 文 件 夹<br>1 无 线 监 视器<br>國 性能日志和警  | 田序(2) ()<br>第元:   | <del>其子(g)</del><br>供应商<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft  | Corpora<br>Corpora<br>Corpora<br>Corpora  | ? |
| 添加 (Q)<br>用的独立管理单元<br>雪型单元<br>雪文引服务<br>可文件夹<br>1 无线监视器<br>冒性能日志和警<br>愚远程复面   | 田FFR (2)  | <del>其子(四)</del><br>供应商<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft                             | Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora   | ? |
| 添加 (Q)<br>用的独立管理单元<br>雪索引服务<br>]文件夹<br>1、文件夹<br>1、大线监视器<br>副性能日志和警<br>圆远程桌面<br>1000000000000000000000000000000000000 | 田(R) (2)  | <del>其手面)</del><br>供应商<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft                 | Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora                                  | ? |
| 添加 (Q)<br>用的 独立管理单元<br>雪索引服务<br>可文件夹<br>扩无线监视器<br>副性能日志和醫<br>動远程桌面<br>可证书版发机构  | HPR (2)   | 关于(B)<br>供应裔<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft              | Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora                       | ? |
| 添加 (Q)<br>用的 独立管理单元<br>雪索引服务<br>) 文件夹<br>1 在総日志和署<br>總远程桌面<br>) 证书版发机构<br>) 证书版发机构<br>) 证书版                          | 田序(g) ()<br>9元:<br>9报   | 关于(B)<br>供应癥<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft                           | Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora                       | ? |
| 添加 (Q)<br>用的 独立管理单元<br>雪索引服务<br>可文线监视器<br>副性能日志和署<br>最远程复面<br>可证书版发机构<br>可证书版发机构<br>可以终端服务配置                         | 田序(g) ()<br>中元:<br>中报   | 关于(B)<br>供应商<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft | Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora | ? |
| 添加 (Q)   | 田原(四)<br>ま元:<br>・<br>・<br>・<br>・<br>・<br>・<br>・<br>・<br>・<br>・<br>・<br>・<br>・ | 关于(g)<br>供应商<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft<br>Microsoft | Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora<br>Corpora | ? |

| ○ 我的用户带户 (1) |  |  |
|--------------|--|--|
| ○計算机株尸(1)    |  |  |
|              |  |  |
|              |  |  |
|              |  |  |
|              |  |  |
|              |  |  |



| 管理单元添加<br>」(S): | 🔁 控制台根节点       | · Ba |
|-----------------|----------------|------|
| 🗊 证书 - 当前用      | 9              |      |
|                 |                |      |
|                 |                |      |
|                 |                |      |
| 描述              | Image00024.jpg |      |

选择"证书",选择"添加(A)"按钮后,根据系统提示完成证书管理单元选择。在控制台管理界面,选择"证书-当前用户",选择"个人", 点击鼠标右键,选择"所有任务",选择"申请新证书…",进行证书 类别选择

| 2 控制台根节点<br>2 证书 - 当前用户<br>百 近书 - 当前用户<br>百 元 (1) | 名称<br>回证书 - 当前用户 |
|---|------------------|
| 田 所有任务 (L) <b>&gt;</b>                            | 查找证书(图)          |
| 田 从这里创建窗口(1)                                      | 申请新证书(图)         |
| ↓<br>→ 局新(E)                                      | 导入(1)            |
| - 帮助(B)   |                  |
| 田 🧰 受信任人<br>田 🥶 证书注册申请                            | -                |



| 证书申请向导 | ×  |
|--------|--|
|        | 欢迎使用证书申请向导   |
|        | 这个向导帮助您从城中的证书感觉机构 (CA)申请新证书。                           |
|        | 由证书假发机构服发的证书是确认您的身份的文件,它含有用来保护数据或建立安全网络连接的信息。          |
|        | 私钥是与证书相关的公钥私钥对中的机态的那一<br>半。可用它来数字签名或解密用相应的公钥加密的<br>数据。 |
|        | 要继续,读单击"下一步",  |
|        |  |
|        | (上一歩の) (下一歩の) 2 取消                                     |

选择"注册代理",选择"下一步(N)>"按钮,根据系统提示填写 出现证书的名称和描述等信息完成注册代理证书的申请

| 証书申请府导  | ×                      |
|---|------------------------|
| 证书类型<br>证书类型包含 <sup>Image00027.jpg</sup> 量的加                            | 《性值-                   |
| 为您的请求选择一个证书类型。<br>问的那些证书类型。   | 5只能访问来自受信任的 CA 并且您有积限访 |
| 证书类型 (C):   |                        |
| EFS 故障恢复代理<br>基本 EFS<br>系統管理员<br>用户<br>智能卡登录<br>智能卡登录<br>智能卡里户<br>提出面貌到 |                        |
| 要选择加密服务提供程序和 CA,<br>厂 函媒 (型)  | 选择"高级"。                |
|   | <上一步@)下一步@) 取消         |
| 证书申请府导  | ×                      |
| <b>证书的好记的名称和描述</b><br>您可以提供名称和描述,以便快速                                   | 识别某个证书。                |
| 力新证书推入好记的名称和描述。<br>好记的名称 (E):<br>[het+eh]                               |                        |
| 描述 (1):   |                        |
|   |                        |
|   |                        |
|   |                        |
|   |                        |
|   | <上步(1)) 下              |



| 19416149<br>19 |  |  |
|----------------|--|--|
|                | 正在完成证书申请向导<br>您已成功地完成了证书申请向导。                              |  |
|                | 您已指定下列设置   |  |
|                | Marging Action Action<br>執戸名 administrator<br>計算机名 VINDCO1 |  |
|                | 证书模板 注册代理 [Image00028.jpg]                                 |  |
|                |  |  |
|                |  |  |
|                |  |  |
|                |  |  |
|                | < 上一步 (b) 完成 取消  |  |

完成注册代理申请后,可以在看到已经颁发给个人的证书的信息

| 5   | ──────────────────────────────────── | 到的 Internet |
|-----|--------------------------------------|-------------|
|     |                                      |             |
| E#S | 使用证书可正确标识您自己、证书颁发<br>身份。             | 成机构和硬发商的    |
| -   | 清除 SSL 状态 © ┃ 〒〒◎<br>言島              | 发行商 ①       |
| È   | 自动完成功能存储了以前的条目并将<br>符合的项目推荐给您。       | 自动完成 (1)    |
|     | Microsoft 配置文件助理能存储您的                | 配置文件(8)     |



| 波给           | 領装者           | RLE E RUE   AF | 记的名称 |
|--------------|---------------|----------------|------|
| Administrate | r hotech i    | 010-5-9 h      | tech |
|              |               |                |      |
|              |               |                |      |
|              |               |                |      |
|              |               |                |      |
|              |               |                |      |
|              |               |                |      |
|              |               |                |      |
| Q)           | 出(12)」 删除(12) |                | 商级(6 |

#### 申请证书



## 选择"高级证书"进行高级证书申请





选择"通过使用智能卡证书注册站来为另一个用户申请一个智能卡证书",出现智能卡证书注册站

| Normalt 🖬 118 6 - Monualt Internet Explorer                        |            | 10 | à |
|--|------------|----|---|
| 文件D 朝鮮D 重新D 年期3 工具D 帮助出  |            |    | ł |
| 3 az - () - 2 🖉 🖓 paz 🕎 ezz 🕘 🔂 🔂                                  |            |    |   |
| titizzo 🕼 tezo (Wendelli, Antest, conclorezo (Antripad esp         | · 🛃 महा    | 69 | 1 |
| Bereart 2484 — Letuk   |            | ŧЯ | 1 |
| 高级征书申请   |            |    |   |
| CA 的價略決定您可以申请的证书关税。单击下列选项之一来:                                      |            |    |   |
| 创建并向此 CA 提文一个申请。   |            |    |   |
| 使用 base64 编码的 CMC 或 PMCS #10 文件建文 一个证书申请, 或使用 base64 编码的 P<br>世申请, | XCS #7 文件读 | TE |   |
| 通过使用智能卡证书注册站来为别一用户申请一个智能去证书。                                       |            |    |   |
| 注意:意必须有一个注册代理过书是为另一 用户提交编末。 [mage00036.jpg]                        |            |    |   |

在弹出的"ActiveX"警告框中,选择"是"

| 121 | 在此面上  | ActiveX | 授件和本で上  | 約其它部份的变 |
|-----|-------|---------|---------|---------|
| 2   | 宣可能不知 | 安全。你想了  | 记许这种交互可 | 1?      |
|     |       |         |         |         |
|     |       |         |         |         |

进入智能卡证书注册站界面后,可以看到相关的一些基础信息

| THE SHAD BOD WALL INT WARD  |     |
|---|-----|
| () SE - () - () () () () () SE - () () () () () () () () () () () () () |     |
| things in http://www.itt.formit.com/ortro/inform.au                     | ·   |
| Figure 1. 225   | 2.8 |
| 智能卡证书注题站  |     |
| 2.540:  |     |
|   |     |
| #2#08/07/   |     |
| (CREALENRY) dame  |     |
| \$\$r   |     |
| 请选择赛注册的用户。  |     |
|   |     |

选择证书模板为"智能卡登录",选择加密服务提供程序为: "FEITIAN ePassNG RSACryptographic Service Provider",选择用户 后,选择"注册"按钮,出现输入用户 PIN 码的对话框



| 也挥用户                            |  |                       |               | ?           | ×        |
|---------------------------------|--|-----------------------|---------------|-------------|----------|
| 选择对象类型(S):                      |  |                       |               |             |          |
| 用户                              |  |                       |               | 对象类型(0)     | 1        |
| 春报位晋(F)·                        |  |                       |               |             | 2        |
| 整个目录                            |  |                       |               | 位置(1)       | 1        |
| 1 () 第34-55(1)34-6-4            | 790-050tes) (#) -  |                       |               |             | 4        |
| 新八支近井町川家(                       | 240 (22011) (2) -  |                       |               | A ME AVA AL | 1        |
| jss (jss@hctech.)               | <u>:on)</u> ]  |                       |               | 检查名称 (C)    |          |
| 高级(4)                           |  |                       | 稳定            | 取消          |          |
| Normal WEIGER, Norm             | all Second Support   |                       |               |             |          |
|                                 | C C RE CORA  | 0.0.00                | 3             | 3 (D *      | er was - |
| licenti (184                    |  |                       |               |             | 1.5      |
| 智能卡证书注册站                        |  |                       |               |             | _        |
| <b>法新选项</b> :                   |  |                       |               |             |          |
| 218204                          | 242<br>7   |                       |               |             |          |
| ME FEIL                         |  | ahie Server Provide 👁 | i i           |             |          |
| THE DOCUMENT                    | data and a second s | - 21k                 | 11.2 t        |             |          |
| ENGINE.                         |  |                       |               |             |          |
| F-0                             | CH12.224   | 298                   | 体而户           |             | _        |
| 85.                             |  |                       | -             |             |          |
|                                 |  |                       |               |             | _        |
| UP PIN 69                       | ≙iŒ  |                       |               |             | ×        |
| <b>《</b> 》<br>现在                | f ePass To<br>E需要验证的   | oken <b>f</b><br>您的用户 | pin 码         |             |          |
| E F                             | PTN:   | www.                  | 200-11 (1958) |             |          |
| 7.57                            |  | 14. N.                | 721           |             |          |
|                                 |  | 确定                    | (Q)           | 取消          | (C)      |
|                                 |  |                       | 8.            |             |          |
| Concession of the Parlie of the | and the second second  |                       |               |             | لم       |
| 3 88 - () = 1 (2)               | 1  | (F (P) (A)+ 3         | ER -34        |             |          |
| AND ME HARD                     | unicense v/centares and  | -                     | 123 49        |             |          |
| Ricconnfr 12484                 |  |                       |               |             | .83      |
| 智能卡证书注册站                        |  |                       |               |             |          |
| 2#84:                           |  |                       |               |             |          |
| <b>这种模称</b> :[91]               | 中政主法   |                       |               |             |          |
| UP HOR MINING - Frank           | 0.2  |                       |               |             |          |
| 图卡语纳拉尔。<br>第12日                 | and effective lifest Dige  | sprattic Sirmin Pro-  | - 31          |             |          |
| 28074 ( L                       |  |                       |               |             |          |
| RARDAP:                         | Potech Law   |                       | Inage00042 jp | 2           |          |
| R.E.:                           |  |                       |               |             |          |
| 智能卡准备好了。 講性 '                   | 查看证书"来请保证  | [书包会用户正确]             | 中个人信息。        |             |          |
|                                 |  |                       |               | 2022        | 1月25日    |
|                                 |  |                       |               |             |          |
|                                 |  |                       |               |             |          |

# 完成证书的导入,然后利用智能卡进行身份验证登录AD域